FEDERAL ENERGY REGULATORY COMMISSION
OFFICE OF ENERGY PROJECTS
DIVISION OF DAM SAFETY AND INSPECTIONS
NEW YORK REGIONAL OFFICE
19 West 34th Street - Suite 400
New York, New York 10001

Office No. (212) 273-5900 **FAX No. (212) 631-8124**

FERC Security Program For
Hydropower Projects

November 18, 2002

Slightly over one year has past since the terrorist attacks on New York, Washington, and Pennsylvania occurred and many changes were consequently made to our responsibilities and requirements in the hydropower industry. Since then, we have evaluated the security of our facilities at a much heightened level of alertness and have taken steps that one year ago would not have been considered necessary. In October 2001, the FERC restricted previously public documents from public access. In November 2001, the FERC assigned FERC jurisdictional dams into three groups relating to "security sensitivity" and created a means of notifying licensees and exemptees of security threats via E-mail. In April 2002, we held our first security and emergency response workshop. In June 2002, the FERC created and distributed the FERC Hydro Security Program. In July and August 2002, we held our first Division of Dam Safety and Inspections Regional Office outreach meetings to acquaint licensees to the security program and to solicit comments. Continuing with our efforts to provide training and information to the hydropower industry, the FERC is coordinating an emergency preparedness/security workshop in conjunction with the 2003 USSD Annual Meeting and Conference in Charleston, South Carolina on the weekend prior to the Conference (April 12-13, 2003).

All of you have assessed the state of your site security as it existed one year ago and made immediate changes as you deemed necessary. Many of you have completed, or are in the process of completing, more detailed assessments of the security at your hydroelectric

projects and will make additional security enhancements as appropriate. So far, the response from the FERC licensees and exemptees has been very professional. As stated in the FERC Hydro Security Program, this new program has been designed to be adaptable so that we all may learn from our shared experiences to revise the program as necessary. The purpose of this letter is to recap where we currently are, clarify what may still be unclear, and discuss how we should proceed in this next year.

There are two enclosures with this letter. Enclosure 1 provides a summary of licensee/exemptee requirements for security concerns and a clarification of what the FERC expects from those requirements. Enclosure 2 includes Revision 1 of the FERC Security Program for Hydropower Projects. Major changes made to the program are summarized on pages 1 and 2 of the enclosed program.

If you have already completed the requirements of the FERC Security Program, please submit to this office, in general terms, the methodology used to complete the assessments, the basis used for the conclusions of your assessments, and when the assessments or plans were completed. If your requirements still need to be completed, please submit to this office a plan and schedule discussing how you will accomplish your security requirements. Note that all requirements must be completed by September 30, 2003. Please provide the information on how the requirements will be completed to this office by December 16, 2002.

Thank you for your continued efforts to evaluate and improve security at the FERC jurisdictional dams. If you have any questions or comments, please contact Charles Goggins at (212) 273-5910.

Sincerely,

Anton J. Sidoti,
Regional Engineer

Enclosure 1

Summary of Licensee/Exemptee Security Requirements and Clarification of Requirements

Security Groupings of Dams

Licensees and exemptees were informed last November of how the FERC distributed FERC-jurisdictional dams into three security groups. You were provided the opportunity to comment on these groupings and some of you requested changes to the groupings. The response from licensees again was very professional. If any requests for grouping changes are still desired, please contact the Deputy Regional Engineer in this office for resolution of those concerns.

FERC Security Inspections

By now, the FERC has completed a security inspection of all High and Significant Potential Hazard Dams, and approximately one-third of the Low Hazard Potential Dams. During this inspection, the Security Checklist Form was completed by the FERC inspector and was fully discussed with the licensee/exemptee representative. From the approximately 1,500 dams inspected, no dams were recommended for major follow-up security actions, which again points to the professional and conscientious work our licensees and exemptees are doing. The Security Checklist Form appears to be working well. One point about the Security Checklist that may not have been clear is that licensees/exemptees may request a photocopy of the completed form at the conclusion of the inspection. If you need a copy of the completed form, or have comments about the form, please contact this office.

Enclosure 1

Summary of Licensee/Exemptee Security Requirements and Clarification of Requirements

Plans and Assessments Required by Licensees and Exemptees

To recap the licensee/exemptee requirements of the revised Hydro Security Program, the following are required:

Requirement	Security Group 1	Security Group 2	Security Group 3
Security Assessment	Yes[1, 4]	Yes[1, 4]	No[2]
Vulnerability Assessment	Yes[1, 5]	No[2, 5]	No[5]
Security Plan	Yes[1]	Yes[1]	No[2]
Integration of Security concerns and EAP procedures	Yes[3]	Yes[3]	No[2]

[1] Completed by September 30, 2003.

[2] Although not required, this item is strongly encouraged.

[3] Integration should begin immediately, and be revised as conditions change and documents are refined or developed.

[4] A separate Security Assessment may not be required for a dam if a more detailed Vulnerability Assessment is completed for that facility that addresses the need for security upgrades.

[5] A Vulnerability Assessment must be completed prior to the FERC approval of requests for permanent closures of recreational, or other project, facilities.

Some of you have completed portions or all of these requirements. Note that the due date of these requirements for existing projects is September 30, 2003. We understand that many licensees/exemptees are uncertain about the scope of what the FERC expects. To alleviate some of these concerns, it is beneficial for licensees/exemptees to submit a plan and schedule for assessments and/or plans, as required. In this way, the FERC can determine if the scope of your planned efforts are appropriate to your project prior to their completion. The following is a clarification of these requirements.

For Vulnerability Assessments (VAs), please refer to Sections 2 and 6 of the Hydro Security Program for specific requirements. To clarify what the FERC expects from a VA, the following is a summary of what a VA for a hydro project should include:

- (Threat) Determine if there are any organizations that have a motive, ability, and presence to attack your dam and quantify their capabilities to some degree. This

should include Al Qaeda, militia, extremists, vandals, insiders, etc. Look at past local history (police records) to help evaluate the situation. You should assess potential numbers of attackers, weapons, vehicles, their resources, intent, potential actions, skill levels and so on for each group. You may need to identify several groups. [If risk analysis is used, assign a decimal number as to the likelihood of attack for each group. For Risk, Low is commonly assigned 0.1, Medium is commonly assigned 0.4, and High is commonly assigned 0.9.]

- (Consequences) Determine the consequences of an attack. Loss of uses (mission) of dam, people at risk, time taken to repair, economics, etc. [If risk analysis is used, assign a decimal number as to the consequences of attack as a matrix for each group identified versus each mission of the dam.]
- (Vulnerabilities) Complete a site survey and identify all the features that are vulnerable. This may be the dam, gates, intake, outlet, generator stators, control room, etc.; essentially everything that will potentially affect the mission(s) of the dam or put people at risk.
- (Security system effectiveness) Evaluate the effectiveness of the current security systems on site. List all features, such as gates/locks/cameras/barriers/alarms, and evaluate what an adversary needs to do to arrive at a vulnerable feature, how long it takes to detect (and verify) the adversary, how long it takes for the adversary to arrive at their target, and how long it takes for an effective response force to arrive. This will indicate if the identified group(s) could be successful in their attack. As an example, if a group with the capability to do harm can accomplish their goal in 30 minutes after detection and verification and it takes 45 minutes to successfully respond, then they may have sufficient time to succeed in their attack and you may lose that function of the dam. This usually indicates that an upgrade to your security is warranted. [If risk analysis is used, assign a decimal number as to the system effectiveness.] This is usually the weak point of the assessment, and often will be the driving factor that needs to be changed. It is impossible to change the threat, difficult to change the vulnerabilities, and almost impossible to change the consequences.
- Determine a "design basis threat" that identifies the most likely mode of attack, path they will take, and what will be targeted. This is what you design for.
- If risk analysis is used, apply your decimal estimates to the following equation,:

  Pa * C * (1-Pe) = R. Pa is likelihood of attack, C is consequences, Pe is system effectiveness, R is risk. This will result in a number from 0 to 1.0. Commonly,

0.4+ is undesirable. The goal is to find a way to reduce this number, which usually is done through security upgrades, to possibly 0.2 or less.

- Prepare a plan to revise your security, or to improve other mitigating actions.
- Identify how your revisions will impact the dam and everyday operations, public opinion, economics, etc.

Many licensees/exemptees have asked the FERC about the RAM-D$^{(SM)}$ methodology that was developed by the Sandia National Laboratories. Although this methodology has been adopted as the methodology of choice by many dam owners, the FERC is not specifically requiring licensees/exemptees to use RAM-D$^{(SM)}$. If RAM-D$^{(SM)}$ (or similar) is used, then the FERC will review if the conclusions are reasonable, and how the conclusions are making the security system more effective. If RAM-D$^{(SM)}$ is not used, the thought processes and assumptions used by the licensees/exemptees will be assessed to determine if they are realistic, and if you have completed a good faith effort to increase security then your product will likely be acceptable. VAs may be completed by in-house personnel, however it is critical that a VA be completed by professionals with knowledge of both dam engineering and security. If you use RAM-D$^{(SM)}$, you will have a series of forms filled out with subjective numbers assigned that leads you to the final recommendations. The forms tell you what to add to security to make your response stronger or more effective.

The Security Assessment is similar to the above, except that you do not need to evaluate the threat likelihood or consequences (refer to Section 2 of the Hydro Security Program for more details). What is covered is to see what security is in place and determine if it is appropriate. Obviously, this is not as detailed and you may miss some considerations, but you are looking to see if you need to upgrade security and how to upgrade it. (This is similar to what the FERC inspectors evaluate during the Operation Inspections, but are more detailed and thorough.) If you only do this, you may have some problems justifying to management the costs of your upgrades, because they may not be based on specific details. Many of you will likely find that the difference between a VA and a Security Assessment as defined by the FERC is not extreme and that a VA is a preferred method regardless of the FERC requirements. If you complete a comprehensive VA (as discussed above), then a separate “security assessment” can be omitted. Therefore, dam owners will be able to forego the "security assessment" requirement for those dams having completed a full VA.

The security plan is essentially the SOP for the dam operator to reference in order to operate the security at the dam. What do the guards do, how do you identify on-site

personnel, where are vehicles parked, do you lock doors/windows, how do you communicate, what are the law enforcement phone numbers, what extra do you do if the threat level increases? Identify training, testing, education, etc. The FERC will check security plans to see that varying threat conditions are addressed properly.

The recovery plan details how you get the mission of the dam back in operation in the shortest/most-economic time frame possible. What are the alternatives? Spare parts, etc.

Integrating all plans essentially is making sure everyone is on the same page. Security personnel should not override emergency procedures, or vice versa. Smooth out all inconsistencies beforehand to be sure the entire response to a terrorist event is seamless.

An addition to the FERC Hydro Security Program in Version 2 is that a Vulnerability Assessment is required (regardless of the Security Group of the dam) if the licensee/exemptee requests a permanent closure of recreational use or other project use at that dam.

Enclosure 2

FERC Security Program for Hydropower Projects
Revision 1 (11/15/2002)

Summary of Changes

This version of the FERC Security Program for Hydropower Projects (Revision 1) is the first change to the Program since it was distributed to licensees/exemptees in 2002. These changes (shown in the text by italics) were made as a result of comments and recommendations the FERC received from licensees and other agencies. The following contains a brief discussion of several changes in the Program (minor editorial changes are not identified here):

PAGES	***SECTION***	***DESCRIPTION OF REVISION 1 CHANGES***
3	*2.0*	*Definition of an Emergency Action Plan added.*
3-4	*2.0*	*Definition of a Security Assessment has been expanded and clarified. The distinction between a Security Assessment and a Vulnerability Assessment has been clarified.*
4-5	*2.0*	*Definition of a Vulnerability Assessment has been expanded and clarified.*
6	*4.2.1*	*FERC Staff responsibilities includes recognition that a Vulnerability Assessment is required for any project where a permanent facility closure is requested.*
6	*4.2.1*	*FERC Staff responsibilities includes recognition that the letter to the licensee/exemptee notifying them of an Operation Inspection will specifically state that the security head be invited to the inspection.*
9	*4.3*	*Clarification that licensees/exemptees ensure that the corporate security officer be involved with all security-associated activities.*
10 and 11	*4.3.2 and 4.4*	*Licensee/exemptee responsibilities includes recognition that a Vulnerability Assessment is required for any project where a permanent facility closure is requested.*
11	*4.4*	*Clarification that a separate Security Assessment document is not needed if the Security Assessment is fully addressed in a comprehensive Vulnerability Assessment document.*
11	*4.4.1*	*New requirements for Unconstructed Projects.*
11-12	*4.4.2*	*New requirements for Unlicensed Constructed Projects.*
12	*4.4.3*	*New requirements for Projects with Dams not owned by the applicant/licensee/exemptee.*
12	*5.1*	*Clarification of threat alerts sent to licensees/exemptees by the FERC*
18-20	*6.0*	*Clarification of the content of a Vulnerability Assessment.*
Encl. 1	*---*	*The format of the Security Checklist altered to include fields for checking off responses.*

Enclosure 2

Background

Accomplished to Date:

- A FERC Alert Notification System has been developed and implemented.
- Where dam owners believed it was necessary, security measures have been implemented or enhanced.
- A list of approximately 200 critical dams has been identified for a higher level of scrutiny (Security Group 1). The remaining High and Significant Hazard Potential Dams have been placed in Security Group 2 and Low Hazard Potential Dams have been placed in Security Group 3. These groupings are subject to periodic review and can change upwards or downwards.
- Coordination with National Hydropower Association (NHA) in identifying and distributing general guidelines for security measures.
- The FERC personnel attended a RAM-D Vulnerability Assessment of a USACE-Baltimore District project.
- Train Key HQ and RO Staff in RAM-D Vulnerability Assessment methodology.
- During the FY2002 operation inspections, the FERC engineers determined if reasonable security measures are in place at all high and significant hazard potential dams.
- Issued Version 2 of FERC Security Program for Hydropower Projects 10/30/2002.

Next Steps:

- Continue and expand training of HQ and RO Staff in vulnerability assessment methodologies.
- The FERC engineers will determine if reasonable security measures are in place at all high and significant hazard potential dams by:
- Reviewing the licensee/exemptee security assessments
- Reviewing the licensee/exemptee response to the security assessments
- Identifying where additional security enhancements are necessary.
- Constantly re-evaluate the program according to current Threat Condition as determined by the Attorney General and the Office of Homeland Security, and adjust where necessary.

Enclosure 2

FERC Hydropower Security Program

1.0 Preface

The Division of Dam Safety and Inspections (D2SI) will be monitoring the security measures being implemented at jurisdictional dams beginning in FY 2002 and continuing for the foreseeable future. This document provides guidance to the FERC staff and licensees/exemptees to perform this program.

2.0 Selected Definitions

The following definitions are used in the FERC Security Program for Hydroelectric Projects:

Emergency Action Plan (EAP) *- A document describing the actions a dam owner/operator takes if a problem exists at a dam, whether due to natural causes or sabotage. Actions include identifying and assessing the problem, mitigating the problem if possible, and notifying the emergency management system to protect human life and property. Inundation studies and notification call charts are included in EAPs.*

Integration of plans - In this program, "integration" of plans is defined as ensuring that there is continuity between the many company documents that may exist, such as Security Plans and Emergency Action Plans (EAPs). Emergency and response actions arising from procedures contained in company documents should be internally consistent, with few if any procedural conflicts. Authors and administrators of documents within a company should ensure that proper coordination has been achieved and, as an example, the security personnel understand the procedures contained in the EAP and vice versa. "Integration" does not mean that security information should be incorporated into an EAP, which would have a wider distribution than a Security Plan.

Recovery Plan - A document describing the actions an organization will take to recover from a disaster. The disaster can be natural or caused by criminal activity. A Recovery Plan in this program generally refers to the pre-planned actions allowing a utility to continue, *or quickly restore*, generation of power, or otherwise function in its intended purpose. This document is also known as Utility Recovery Plans, Continuity of Operation Plans, etc. This document can be specific to a hydropower dam or reservoir, and/or part of the entire utility company recovery plan.

Security Assessment - An evaluation of *the current state and appropriateness of the on-site security system and* what needs to be done at a project or facility to address concerns

regarding security, such as installation of fences, gates, cameras, increased guards, etc. *This assessment will identify if any security enhancements are needed, and specifically what those enhancements consist of. The recommendations made from the Security Assessment will lead to improved security measures and should be incorporated into the corporate Security Plan (see definitions, below).* The level of response is highly dependent upon several factors, such as site-specific characteristics of the project, anticipated threat, changing level of local, regional, or national threat alerts, etc. A Security Assessment is often preceded by, or incorporated within, a comprehensive Vulnerability Assessment. *Factors determined from a Vulnerability Assessment (see definitions, below) will greatly assist with the proper evaluation of site security, and will often lead to a more-informed security assessment decision. Without knowledge of the factors evaluated in a Vulnerability Assessment, there is a greater risk of not identifying all vulnerable features, or of recommending security enhancements that are not comprehensively integrated with the entire project site. Security Assessments are required for Security Group 1 and 2 Dams, and are stand-alone documents or can be incorporated within a more detailed Vulnerability Assessment. Refer to section 4.4 for additional details. The main difference between a Security Assessment and a Vulnerability Assessment as defined in this guidance is that the Vulnerability Assessment provides a detailed decision-making process leading to what needs to be protected, what it should be protecting against, how effective the security system currently is, and what the consequences of an attack against the facility will be, whereas the Security Assessment evaluates the current security system and recommends if and how the security system can be enhanced.*

Security Plan - A document that characterizes the response to security concerns at a project or facility. The Security Plan may include specific features of the project security program, such as fences, surveillance cameras, etc. and company procedures to follow based upon changing threat conditions or situations. The Security Plan can be very simple or very complex based upon the specifics of the site as well as the assessment of the potential threat to the facility.

Vulnerability Assessment - A Vulnerability Assessment (VA) *addresses the following four factors*: 1) it identifies the "weak points" or vulnerable project features at a facility; 2) it assesses the potential threat to a facility as based on organizations or people (including locals) who may wish to cause harm to the facility, a history of security incidents, and information received from the FBI or other *law enforcement* agencies *specific to your area or facility; 3) it addresses* the consequences of such an attack, *and; 4) it addresses the effectiveness of the security system to counter such an attack. These factors should be addressed with a fair degree of confidence, with some supportive documentation to substantiate the assumptions. VAs must be completed for all Security Group 1 Dams, and for any dams where there is a request to permanently (in excess of 30 days) close*

usage (i.e., recreation or roads) of project lands for security reasons. A Security Assessment (see definition, above) may be incorporated within a detailed VA. Refer to sections 4.4 and 6.0 for additional details.

3.0 Objective

As one of the special focuses of the Operation Inspections, by the end of the FY 2002 inspection season, the FERC Dam Safety staff completed inspections to determine if reasonable security measures were in place at all High and Significant Hazard Potential dams. Once reasonable measures are in place, the FERC Dam Safety staff will continue to periodically monitor the security measures at jurisdictional hydropower projects against the current threat conditions as determined by the Attorney General and the Office of Homeland Security to determine if the licensees/exemptees have a plan to alter the level of response and preparedness as appropriate and as conditions evolve. The reasonableness of security measures at all Low Hazard Potential dams will be reviewed as they are scheduled for Operation Inspections over the inspection scheduling cycle.

4.0 Requirements and Responsibilities

4.1 General Requirements

Security measures taken at hydropower facilities are the responsibility of the licensee/exemptee. The FERC Dam Safety personnel will assist licensees/exemptees when requested, or provide points of contacts to those requesting further information. The FERC Dam Safety staff will monitor what actions are being made at jurisdictional dams and will comment on the appropriateness of those measures specific to the facility. What appear to be deficiencies will be discussed with the licensee/exemptee to arrive at a mutually agreed to response. The FERC Dam Safety staff should recognize that the current level of threat or warning may result in varying response actions from the licensee/exemptee. Therefore, at heightened threat conditions, the licensee/exemptee may need to strengthen the on-site response, whereas at lower threat conditions, relaxation of some security measures may be appropriate. The overall level of security will vary due to site-specific conditions.

The FERC Hydropower Security Program is designed to be adaptable. As the national situation evolves, and the FERC receives comments from licensees/exemptees, the program can be adjusted as necessary. As we all gain experience with these issues the FERC will continue to discuss the security program in periodic meetings with licensees/exemptees to determine any necessary, coordinated, revisions to the program.

4.2 FERC Staff Responsibilities

The FERC staff will be responsible for:

- Conducting initial meetings with licensees/exemptees to discuss the security program.
- Review, monitor, audit, recommend, and evaluate security measures at projects as part of regularly scheduled operations inspections.
- Determine if the actions of the Emergency Action Plan (EAP), Security Plan, and Recovery Plan for all projects that have those documents are integrated.
- Require Vulnerability Assessments of Security Group 1 Dams and security assessments at Security Group 1 and 2 Dams.
- Communicate threat alerts and threat information from nearby and similar projects to licensees/exemptees.
- Protect information regarding security at projects from public disclosure.
- Review security measures for conflict with License requirements.
- Hold annual seminars to discuss the progress of the security programs.

4.2.1 FERC Staff Responsibilities During Operation Inspections

Security will be discussed at all Operation Inspections during FY 2002 and beyond. All Significant and High Hazard Potential Dams were evaluated as to the reasonableness of the security measures in-place by the conclusion of FY 2002. A security checklist to be used during the inspection is included as Enclosure 1.

The FERC staff will also review how upgraded security elements impact license articles, especially relating to environmental concerns and recreation. Any closures of facilities, such as for recreational areas *or roads*, exceeding 30 days may need to proceed through the license amendment process. Permanent closure of *license-required* facilities should not be allowed without license amendment. *In addition, requests for permanent facility closures will require the completion of a Vulnerability Assessment to assess the situation and to determine the appropriateness of such actions*.

During the Operation Inspection, security matters will be discussed with the appropriate licensee/exemptee personnel. The person responsible for security at the facility, or other appropriate personnel, should be present during the security discussions. *The letter to the licensee/exemptee notifying them of the upcoming inspection should clearly state that the security head be provided the opportunity to attend the inspection*. Documentation of the security overview is discussed in the next section.

Items to review during the inspection are included in the Security Checklist

(enclosed). Security details can be discussed during the inspection, however the FERC inspector will not prescribe requirements for specific security hardware additions or modifications at the time of the inspection. The FERC inspector will review the overall appropriateness of the security response, rather than the details. Recommendations, or suggestions, can be offered to the licensee/exemptee for their consideration. Completed Security Checklist forms will be done by hand only and will not be prepared by electronic (computer) means at any time.

If a project has a written Security Plan, security assessment, or Vulnerability Assessment, the FERC inspector will look at the documents and will determine if the security in place during the inspection is appropriate and if the observed procedures are consistent with the current state of threat and is consistent with what is contained in the plans. If there are no written plans, then the FERC inspector will ask the operator how their organization determines and judges the effectiveness of their security response. Some plans are required for Security Group 1 and 2 dams (see section 4.4 for details).

4.2.2 FERC Operation Inspection Documentation and Follow-up

Responses are to be recorded by the FERC engineer conducting the inspection (using the Security Checklist as a guide) and discussed with the site personnel. As much as possible, comments will be fully discussed with the on-site personnel to provide them the opportunity for interactive feedback. Security recommendations made in the field will be of a generic nature.

Upon return to the office, the FERC engineer will submit and discuss the recorded data with the Lead Engineer and Deputy Regional Engineer. For Security Group 1 Dams, a FERC Task Group will review all FERC staff recommendations to ensure that national consistency is maintained. Any necessary follow-up actions would be communicated to the licensee/exemptee by direct communication via telephone and recorded (by hand only) in a telephone memo that would be included with the checklist. If the Security Checklist form has the "Security Measures appear to be reasonable: Yes" box checked, then no follow-up telephone memo is required and the issue is closed. If the Security Checklist form has the "Security Measures appear to be reasonable: No, follow-up actions will be made" box checked, then a follow-up telephone conference will be made and recorded via a telephone memo that will be placed in the written record along with the Security Checklist. Electronic versions of any materials produced by Dam Safety staff containing security matters for a specific project will be erased from computer hard drives connected to a network, and only one paper copy (and computer removable disk, if necessary) will be retained (see next paragraph for retention details).

All written documentation and computer removable disks of all security issues will

be placed in a project folder and filed in a secure location (locked file or safe) with the Regional Engineer, separate from the general files. This folder will contain the security response correspondence already received from the respective licensees/exemptees, the most recent Security Checklist, and any subsequently related correspondence or telephone memos, and pertinent field notes. The folder will contain only the most recent security data and the previous year's data could be destroyed, as a new updated one is prepared. If any correspondence or e-mails arise from our Security Checklist, the FERC would adhere to retaining all copies of such outgoing and incoming correspondence in this secure file. Specific details about the security measures at a facility will not be conveyed by the FERC Dam Safety staff via e-mail. Specific details about the security measures at a facility are not to be recorded by the FERC Dam Safety staff by any means other than by the Security Checklist. No copies of generated data arising from the FERC Security Program will be sent to *FERRIS (formerly* RIMS).

The Operation Inspection Report will include a statement that security has been discussed and reviewed by the FERC staff. No additional details will be provided in the Operation Inspection Report. Suggested wording for the Operation Inspection Report is as follows:

"Project security was discussed during the current Operation Inspection and any follow-up was provided as needed."

These instructions should be conveyed to the licensee/exemptee personnel during the inspection so that they have an understanding of how the data will be treated.

4.2.3 FERC Staff Review of Security Submissions

In addition to the FERC responsibilities during inspections, the Regional Offices may periodically receive telephonic or written requests to review or approve upgraded security systems, such as fencing, surveillance hardware, etc. The FERC staff should request from the licensee/exemptee an assurance that those additional systems do not conflict with existing license articles or requirements. If there could be a conflict (such as recreational restrictions or conflict) the details of the request should be reviewed on a case-by-case basis. In general, the FERC staff should be reluctant to refuse or alter any security upgrades. However, coordination with DHAC may be necessary depending on the scope of the request. All proposed FERC refusals or alterations to security upgrade requests must be coordinated with the FERC-HQ.

4.2.4 FERC Staff Training

The FERC Dam Safety personnel will be trained with the state-of-the-art of vulnerability assessment/threat assessment/alert technology relating to hydropower facilities. Periodic in-house guidance from the FERC Dam Safety-HQ will be provided as necessary. It is anticipated that annual seminars will be held for the FERC and licensee/exemptee personnel to discuss the progress of the security program, with individual input from licensees/exemptees. As part of initiating the FERC security program, meetings will be held in the FERC regional offices with licensees/exemptees to discuss the program in detail. As part of the learning process, the FERC plans to actively interact and coordinate with other entities having similar security and dam safety programs, such as the EEI, NDSRB, ASDSO, NHA, EPRI, Bureau of Reclamation, TVA, Corps of Engineers, etc.

4.3 Licensee/Exemptee Responsibilities

Licensees/exemptees will be responsible for:

- Security at their projects, vulnerability and risk assessments of their projects (as appropriate), security upgrades, and communicating with local law enforcement and nearby dam operators.
- Having a single designated contact to receive FERC security alerts.
- Having a designated contact to the FERC for other security related communications.
- *Ensuring that the corporate security officer be involved with all security-associated activities*.
- Making sure that security measures do not conflict with License requirements.
- Integrating the EAP, Security Plan, and Recovery Plan for their projects, if that project has those documents.
- Communicating to the FERC Dam Safety staff and nearby dam operators regarding security breaches or incidents, if not expressly restricted by law enforcement agencies.

4.3.1 Licensee/Exemptee Responsibilities During Inspections

Licensees/exemptees will be expected to appropriately augment on-site inspections of project facilities in light of security. The frequency of "walk-downs" and the control of public visitors and project users should be evaluated. Special attention should be made to observe suspicious activities and "danger signs" from vulnerable project features or potential failure modes, including visual signs of distress and critical instrumentation readings. "Trigger points" for action arising from critical instrumentation should be defined.

4.3.2 Licensee/Exemptee License and Recreational Responsibilities

Interruptions to recreational and project use should be minimized to the greatest extent possible. However, temporary (i.e., 30 days or less) restrictions may be appropriate in certain circumstances. Measures affecting recreation and project use in excess of 30 days duration must be coordinated with the FERC Regional Office prior to implementation. *Requests for permanent facility closures will require the completion of a Vulnerability Assessment to evaluate the conditions and determine whether the permanent closure is justified, or whether modifications to project use plans are more appropriate.*

4.4 Licensee/Exemptee Requirements

The FERC Hydropower Security Program will be administered on a three-tiered basis, as determined by the Security Grouping to which the dam belongs. Dams belonging to Security Group 1 will be inspected with a high level of scrutiny by the FERC Dam Safety staff. Security Group 1 and 2 Dams are required to have a written Security Plan (see "2.0 Definitions"), and it is suggested that Security Group 3 Dams also have a written Security Plan. In addition, the licensee/exemptee for a Security Group 1 Dam will be expected to place more emphasis on security than for Security Group 2 or 3 Dams, and are required to have a written Vulnerability Assessment *by September 30, 2003* (see "6.0 Vulnerability Assessments" below for further requirement details).

The remaining High and Significant Hazard Potential Dams (Security Group 2) will also be inspected by the FERC Dam Safety staff at a high level of awareness, consistent with the potential threat level. However, Security Group 2 Dams will not be required to have a Vulnerability Assessment (see "2.0 Definitions") completed, but must have completed a Security Assessment by September 30, 2003 (see "2.0 Definitions"). In addition, the expected response to changing threat conditions at a Security Group 2 Dam may not be as stringent as for dams of Security Group 1.

Low Hazard Potential Dams (Security Group 3) will be inspected as they come up for inspection, on the approximate 3-year cycle. Security at Low Hazard Potential Dams will be highly dependent on the opinions of the licensee/exemptee, and the FERC recommendations at Low Hazard Potential Dams should be minimal. In addition, Vulnerability Assessments are not required for Security Group 3 Dams, and the expected response to changing threat conditions may be fairly minimal. Security Assessments for Security Group 3 Dams are highly recommended.

Although some FERC-jurisdictional dams are exempted from EAP requirements, it is suggested that some consideration be given to the emergency response arising from

security breaches at dams without EAPs.

The requirements for FERC jurisdictional dams are summarized in the following table.

Requirement	Security Group 1	Security Group 2	Security Group 3
Security Assessment	Yes[1,4]	Yes[1,4]	No[2]
Vulnerability Assessment	Yes[1,5]	No[2,5]	No[5]
Security Plan	Yes[1]	Yes[1]	No[2]
Integration of Security concerns and EAP procedures	Yes[3]	Yes[3]	No[2]

[1] Completed by September 30, 2003.
[2] Although not required, this item is strongly encouraged.
[3] Integration should begin immediately, and be revised as conditions change and documents are *refined or developed.*
[4] A separate Security Assessment may not be required for a dam if a more detailed Vulnerability Assessment is completed for that facility that addresses the need for security upgrades.
[5] A Vulnerability Assessment must be completed prior to the FERC approval of requests for permanent closures of recreational, or other project, facilities.

4.4.1 Unconstructed Projects

The licensee/exemptee requirements as described in section 4.4 (above) for unconstructed projects must be completed no later than 60 days before the initial filling of the project reservoir begins.

4.4.2 Unlicensed Constructed Projects

An unlicensed constructed project (existing dam or other appurtenant structures) is one where an application for license has been filed or one that has been determined to be jurisdictional by the Commission. Such projects must have the requirements as described in section 4.4 (above) completed no later than the earliest of: 1) six months after the date the license application is filed; 2) six months after the Commission issues an order determining that licensing is required, or; 3) a date specified by the Commission or its authorized representative.

4.4.3 Projects With Dams Not Owned by the Applicant/Licensee/Exemptee

When the applicant, licensee or exemptee is not the owner of the dam nor is otherwise responsible for the maintenance, operation and monitoring of the dam, the applicant, licensee or exemptee should coordinate with the dam owner to ensure that security is appropriately addressed. If the owner of the dam (not subject to the FERC dam safety regulations) refuses to cooperate with the applicant/licensee/exemptee, then the appropriate Federal or State Dam Safety Official will be contacted be the FERC and a meeting established to resolve the situation.

5.0 Threat Alerts and Communications

5.1 FERC Staff Communications

In addition to threat alerts issued by the Office of Homeland Security or the National Infrastructure Protection Center (NIPC), appropriate threat alerts and other security communication matters will be provided to licensees/exemptees by the Regional Office with guidance from the FERC-HQ for national consistency. Special email groups have been established in each FERC Regional and HQ Office. Communication will be handled primarily through the use of email for those licensees/exemptees with email addresses, and via fax or telephone for those without email or those who request multiple communication mechanisms. Follow-up telephone calls to Security Group 1 Dam owners may be appropriate, depending on the urgency of the alert. *This is currently the best system for contacting all licensees, particularly for those who do not have access to the National Electric Reliability Council (NERC) alert system. Threat alerts will be as specific as possible, and all licensees/exemptees will receive the alert regardless of the security grouping of their facilities. The standard format for the alert is as follows:*

> ***"Please respond back via E-mail reply that you have received this message:***
>
> ***Security Threat Alert:***
> ***The (organization) has issued the following security notice on (date/time):***
> ***'…message…'***
> ***Considering the information in our letter to you dated November 21, 2001 please take notice of this alert and evaluate the current status of your security at all your hydro-related facilities in accordance with their Security Group established in that letter and ensure that the level of security at these facilities is appropriate for this security alert."***

The FERC Regional Offices will report security incidents to the FERC-HQ, who will report, as appropriate, to other FERC Regions and others entities with similar security

and dam safety concerns.

5.2 Licensee/Exemptee Communications

Unless specifically restricted to do so by law enforcement agencies, licensees/exemptees should report any security incidents to their FERC Regional Office, which in turn may be passed on to other licensees, especially in the immediate area of the incident. Licensees/exemptees should also maintain very close communication and cooperation with other dam owners in their drainage basin. If a security situation arises at their facility that could affect other dam owners, then those affected dam owners should be notified as quickly as possible by the licensee/exemptee to provide a coordinated emergency response and/or to protect other facilities. Dam operators should inform local law enforcement personnel that security-critical information obtained from one facility should be passed on to other dam owners in the area, and should educate them as to the potential negative implications of not informing upstream or downstream facilities of local emergencies. The licensee/exemptee should offer to assist local law enforcement in this matter.

Procedures for communication must be established between the dam operator and local law enforcement agencies. Telephone numbers should be posted in conspicuous locations to ensure that the time taken to respond to an emergency is minimized. Face-to-face meetings are strongly suggested, and an on-site orientation of project facilities for local law enforcement personnel may be very beneficial to *the overall emergency response*.

5.3 National Threat Alerts and Example Licensee/Exemptee Response Actions

On March 11, 2002 the Office of Homeland Security issued a National Threat Warning System (Homeland Security Presidential Directive-3) with five Threat Conditions, each identified by a description and corresponding color, ranging from lowest to highest as:

- Low = Green;
- Guarded = Blue;
- Elevated = Yellow;
- High = Orange;
- Severe = Red.

The following response actions are provided as examples to licensees/exemptees for their consideration to implement as based upon the current Threat Condition. These examples are not meant to supercede any existing procedures contained in specific Project Security Plans, but rather serve as examples of what could be implemented.

5.3.1 Green (Low) Alert

Low risk of terrorist attacks. There is no credible evidence of a potential terrorist attack against a hydroelectric facility in the United States or regional area. The following protective measures can be considered:

1. EMPLOYEES

- **$** Perform background checks (level of detail determined by the licensee/exemptee) on any employees who could affect hydropower operations.
- **$** Keep personnel informed of alert levels and, at regular intervals, remind all personnel to report the following to appropriate law enforcement or security personnel.
    - A. Suspicious personnel observing, photographing, or asking questions about dam operations or security measures.
    - B. Unidentified vehicles parked or operated in a suspicious manner on, or in the vicinity, of Project facilities.
    - C. Suspicious parcels or packages.
    - D. Any other activity considered suspicious.

2. PLANNING AND COORDINATION

- **$** Regularly review and modify security plans and recovery plans (if present), and EAPs. Keep emergency contact lists up to date, coordinate with local law enforcement and security agencies and ensure that they are familiar with facility locations and operations.

3. SITE SECURITY

- **$** Maintain appropriate level of site security. Secure buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities and areas at the facility or activity level.
- **$** Provide routine surveillance of visitors, tour groups, and other public users of Project facilities and lands.

5.3.2 Blue (Guarded) Alert

Guarded risk of terrorist attacks. There is no credible information to suggest a potential terrorist attack against a hydroelectric facility in the United States or regional area, but a potential may exist. In addition to the previous measures, the following protective measures can be considered:

1. EMPLOYEES

$ Communicate the alert level to employees; remind them more frequently to report all suspicious or unusual activities.

2. PLANNING AND COORDINATION

$ Review all operations plans and orders, EAPs, Recovery Plans, and Standard Operating Procedures (SOPs) that pertain to implementation of Alert Levels Yellow, Orange, and Red.

$ Increase liaison with local police, intelligence and security agencies to monitor the threat to Project personnel and facilities. Notify local law enforcement agencies concerning measures that, if implemented, could impact on their operations in the local community.

$ Consider the use of emergency exercises and drills to enhance overall preparedness.

3. SITE SECURITY

$ Regularly inspect all buildings, rooms, and storage areas not in regular use.

5.3.3 Yellow (Elevated) Alert

Elevated risk of terrorist attacks. There is no credible information to suggest a potential terrorist attack against a hydroelectric facility in the United States or regional area, but there is a general concern of terrorist activity. In addition to all the previous measures, the following protective measures can be considered:

1. EMPLOYEES

- **$** Inform personnel of the general threat situation. Frequently update personnel on changing conditions and inform them of unclassified threat information, if available, and continue to stress the importance of vigilance.
- **$** Consider the implementation of random identity checks (inspection of identification cards, security badges, and vehicle registration documents).

2. PLANNING AND COORDINATION

- **$** Review provisions of all operations plans and orders, EAPs, Recovery Plans, and SOPs associated with implementation of Alert Levels Orange and Red.
- **$** Notify all law enforcement personnel, guards, and security augmentation force personnel concerning the current situation.
- **$** Increase liaison with local police, intelligence and security agencies to monitor the threat to Project personnel and facilities. Notify local police agencies of Alert Levels Orange and Red measures that, if implemented, could impact on their operations in the local community.
- **$** Inform the public of any changes in public access to facilities, visitor centers, and recreation areas.

3. SITE SECURITY

- **$** Reduce the number of access points for vehicles and personnel consistent with the requirement to maintain a reasonable flow of traffic.
- **$** Consider limiting public access to some or all project areas. Consider screening all persons entering visitor centers.
- **$** Consider implementation of 24/7 surveillance of all "critical" facilities (Security Group 1 or others) as necessary. This measure includes unarmed guard forces, armed guard forces and/or law enforcement personnel. Position guard force personnel and/or security patrols at all critical areas. (This measure is especially appropriate in response to specific threat information.)
- **$** Move motor vehicles, heavy equipment, and objects such as trash containers and crates at least 75 feet from critical areas. If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures in accordance with local plans.
- **$** Regularly inspect all buildings, rooms, and storage areas not in regular use.
- **$** At the beginning and end of each workday and at frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, or for signs of tampering, or indications of unauthorized entry.
- **$** Implement screening procedures for all incoming deliveries and official mail to identify possible explosive or incendiary devices, or other dangerous material. (This measure is especially appropriate in response to specific threat information.)
- **$** Install additional physical security measures (barricades, fences, cameras, etc.) as deemed necessary.

5.3.4 Orange (High) Alert

High risk of terrorist attacks. There is credible evidence of a potential terrorist attack against a hydroelectric facility in the United States or regional area. In addition to the previous measures, the following protective measures can be considered:

1. EMPLOYEES

- **$** Provide employees with as much information as possible on threat conditions, update information frequently. Permit variations in work schedules.
- **$** Verify the identity of all employees and authorized personnel entering Project facilities. Inspect identification cards, security badges or other forms of personal identification. Consider implementing a detailed inspection for all entering vehicles (trunk, undercarriage, glove boxes, etc.), suitcases, briefcases, and other containers.

2. PLANNING AND COORDINATION

- **$** Maintain continuous liaison with local police, intelligence and security agencies to monitor the threat to Project personnel and facilities.
- **$** Consult with local or State authorities about closing public roads and facilities that may make Project facilities more vulnerable to attacks. Keep public informed of restricted access and road closings.

3. SITE SECURITY

- **$** Implement 24/7 surveillance of all "critical" facilities (Security Group 1). This measure includes unarmed and/or armed guard forces, and/or law enforcement personnel. Position guard force personnel and/or security patrols at all critical areas. This measure may be augmented by law enforcement agencies, particularly in otherwise unprotected areas.
- **$** Erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.
- **$** Reduce facility access points to an absolute minimum necessary for continued operation. Close all visitor centers and restrict public access to all Project facilities.
- **$** Remove all motor vehicles and heavy equipment parked within 75 feet of critical areas and other sensitive activities specified in local plans. Implement centralized parking and shuttle bus service, where required.
- **$** Where practicable, remove signs that identify the facility.
- **$** Conduct unannounced security spot checks (inspection of personal identification; vehicle registration; and contents of vehicles, suitcases, briefcases and other containers) at access points for Project facilities.
- **$** Cancel non-essential deliveries.
- **$** Cancel non-essential maintenance/construction that utilizes non-company workers.

5.3.5 Red (Severe) Alert

Severe risk of terrorist attacks. An actual attack has occurred against a hydroelectric facility or there is credible evidence that such an attack is imminent. In addition to the previous measures, the following protective measures can be considered:

1. EMPLOYEES

- **$** Verify identity of all employees entering facility, conduct detailed inspections of their vehicles, briefcases, boxes and any other type of containers. Consider options of alternate work sites for essential employees where feasible.
- **$** Keep personnel on duty fully informed of threat conditions, implement means to provide necessary information to employees not on duty.

2. PLANNING AND COORDINATION

- **$** Continue all essential coordination efforts from previous alert levels. Inform public that all facilities are closed. Request that local authorities close those public roads and facilities in the vicinity of Project facilities that may facilitate execution of an attack.
- **$** Contact armed forces for potential coordination efforts in event of attack.

3. SITE SECURITY

- **$** Augment law enforcement and guard forces to provide 24/7 surveillance and ensure absolute control over access to the facility. Implement frequent inspections of the exterior of buildings (to include roof areas) and parking areas.
- **$** Restrict public access to all facilities.
- **$** Inventory and verify the identity of vehicles parked at a facility and move those that are not authorized.
- **$** Thoroughly inspect all items (baggage, suitcases, packages, and briefcases) brought to the site for the presence of explosive or incendiary devices, or other dangerous items.

As the Threat Condition changes (upward or downward) the response at Project facilities can likewise change to meet the current conditions.

6.0 Vulnerability Assessments

A Vulnerability Assessment (VA) *addresses four important factors. The first factor is the identification of the "weak points" or vulnerable project features at a facility. It is important to not only assess the vulnerability of the entire dam and powerhouse, but to also assess vulnerabilities of specific project features, such as*

spillway gates, turbines, etc. The overall effectiveness of the on-site security system can more intelligently be developed and possibly enhanced by identifying all vulnerable features so that a coordinated and comprehensive security system is designed.

A second factor to assess in a VA is the potential threat to a facility as based on organizations or people (including locals) who may wish to cause harm to the facility. *Along with assessing the likelihood that these groups or individuals actually have intent to attack a facility, the capabilities of the groups should be considered to determine if a successful attack is actually feasible. The advantage of trying to assess the likelihood of attack is that resources may actually not be needed if the threat is really not present, or that less detailed security enhancements may be appropriate if the threat is not significant*.

A third factor to address is the consequences of such an attack. *The consequences of an attack on the facility should include the potential for loss of life and of disruption of the services provided by the facility, such as for power generation, water supply, etc. Consequences should be considered for failure of the dam and for failure of vulnerable project features, such as spillway gates, turbines, penstocks, etc. If all potential consequences arising from realistic attack scenarios are low, then the resulting security response will not be as significant as for a project with medium or high consequences.*

The fourth factor to consider evaluates the effectiveness of the site security system against the anticipated adversary attack scenarios to determine if the current security system is adequate. The following security items should be addressed: 1) the ability to detect an intruder; 2) the capability to assess the detection to determine if the detection is a real threat; 3) the ability of the security system to delay the intruder, and; 4) the time taken for law enforcement to respond to the intruder. If the security system is judged to be deficient, then recommended enhancements to security should be made. These recommendations to security enhancement can be made within the VA, or could be determined in a separate Security Assessment (refer to the definition section, above for additional details).

Risk Analysis is often completed in conjunction with a VA and may or may not be appropriate for a facility, as determined by the licensee/exemptee. VAs are to be completed by the licensee/exemptee for all Security Group 1 Dams by September 30, 2003. A multi-person team approach, consisting of several technical disciplines and a security expert, has been found to be the best way to complete VAs at dams. The format, scope, and details of the VA should be determined by the licensee/exemptee, but should be sufficient to address the pertinent vulnerabilities of the project. Security VAs for the remaining High and Significant Hazard Potential Dams (Security Group 2) are encouraged.

In *summary*, a VA *must* contain a discussion of the following items:

- **$** Identify and assess the potential threats (likelihood of attack and adversary types).
- **$** Identify vulnerable facilities and features of a project.
- **$** Determine consequences arising from the implementation of undesirable events.
- **$** Evaluation of the effectiveness of the system to thwart undesired events and adversary types (system effectiveness).

If Risk Analysis is desired by the licensee/exemptee, a suggested general risk equation is provided below, although any method is acceptable (source: RAM-D^{SM}, Sandia, August 2001):

(P_A) * (C) * ($1-P_E$) = R

Likelihood of attack * Consequence * (1-System effectiveness) = Risk

7.0 Integration of Security Procedures with the EAP and Recovery Plan

Security Plans or procedures should be fully integrated with the project Emergency Action Plan and Recovery Plan. Specifics regarding security protocol or on-site security features should not be included within the EAP document, however operating personnel should be fully aware that any dam safety emergency arising from a security concern is to be addressed through the procedures for notification contained within the EAP. The transition from security concern to EAP implementation should be smooth. If the licensee/exemptee has a dedicated security officer, that person should be made aware of the EAP procedures and should provide comments to the EAP coordinator if any procedures could conflict with security protocols. Any conflicts must be resolved.

Recovery Plans should also address security, with a discussion of what it would take to bring a project back on-line for power generation, including but not limited to stockpiles of materials, location of heavy equipment, warehousing critical spare parts, etc. Interruptions to transmission lines and switch yards should be considered.

8.0 Computer Security

During the Operation Inspections, the FERC Dam Safety staff will inquire about measures taken by the licensee/exemptee regarding computer security, communications, and remote operation of project facilities. Discussions should be made to ensure that proper coordination has been made with authorities, such as the FBI Infragard Program. The FBI maintains an incident database and works with those that depend on computer-controlled systems for operations and coordinates activities and technical needs to protect such systems. Therefore, computer-controlled systems are to be updated consistent with state-of-the-art practice.

Enclosure 2

ENCLOSURE 1: FERC Hydro Security Checklist

FERC HYDRO SECURITY CHECKLIST

Project No.:_____ **Project Name:**_____ **Dam:**_____.

Owner:_____ **Security Group:**_____ **Date:**_____.

Inspector:_____ **Accompanied by:**_____.

Field Observations: (Provide additional details on back of sheet, if necessary)	**Y**	**N**	**NA**
1. Is the dam site fenced with gates/doors locked?_____			
2. Is access to the dam/facilities restricted? Foot?_____			
Vehicle?_____			
Boat?_____			
3. Is site manned? Dam: Days/week_____ Hours/day_____			
Powerhouse: Days/week_____ Hours/day_____			
4. Are there surveillance cameras? Dam?_____			
Powerhouse?_____			
Other?_____			
How are they viewed/checked?_____			
5. Are spillway/gate controls secured against unauthorized access?_____			
6. Are powerhouse doors/windows locked?_____			
Alarms/cameras?_____			
Can alarms be easily bypassed? _____			
7. Water conveyance system: Access restricted?_____			
Surveillance?_____			
8. Is there HAZMAT/fuel storage on-site?_____			
Is access secured?_____			
9. Is critical performance monitoring equipment secured against tampering?_____			
10. Are critical drawings/plans/records secured from unauthorized access? _____			
11. Are law enforcement phone numbers posted?_____			

Discuss with owner's representative: (Provide additional details on back of sheet, if necessary)

12. Describe assessment of potential threats, vulnerable facilities and potential impacts. Include switch yards and transmission lines, etc. Also consider any elements of operations that could be subject to cyber attack._____.

13. Steps taken to improve security: **Short term** (immediately following 9/11 attacks):_____.

Long term:_____.

14a. Is there a Security Plan (Group 1 or 2 required by 9/30/03)_____			
Are there different response levels?_____			
Are the measures on the day of inspection consistent with the current threat level?_			
14b. Is there a Vulnerability Assessment? (Group 1 VA required by 9/30/03)_____			
14c. Is there a Security Assessment? (Group 1 or 2 SA required by 9/30/03)_____			
14d. Security actions integrated with EAP? (Group 1 or 2 required immediately)_____			
15. How long would it take to respond to unauthorized access?_____			
What is that response?_____			
16. Can law enforcement be quickly notified?_____			
Estimated time of arrival:_____			
17. Do any security measures conflict with any license requirements?_____			
18. Is frequency of walkdowns appropriate?_____			
Personnel control/ID badges?_____			
19. Computer security has been addressed and is being coordinated with authorities __			
20. Security Measures appear to be reasonable:_____			

If "No", follow-up actions will be made_____

This form will not be made part of any public record and will be retained in a locked file in the FERC Regional Office.

Item No.	Additional Details