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

June 7, 2002

Dear :

Beginning this year (2002), the Division of Dam Safety and Inspections (D2SI) will be monitoring the security measures being implemented at jurisdictional dams. Guidance describing the FERC Security Program for Hydropower Projects is enclosed. This Security Program has been developed through a cooperative effort among D2SI, several licensees, consultants, and other federal agency reviewers. This program has been designed to be flexible and easily modified as our national response to terrorism evolves. It has also been designed to provide licensees/exemptees with as much freedom as possible in making specific decisions affecting the security of their facilities.

As one of the special focuses of the Operation Inspections, by the end of the FY 2002 inspection season, D2SI will complete inspections to determine if reasonable security measures are in place at all High and Significant Hazard Potential jurisdictional dams. Once reasonable measures are in place, D2SI will continue to periodically monitor the security measures at jurisdictional hydropower projects in coordination with licensees/exemptees 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 inspected during the normally scheduled Operation Inspections. Enclosed is the special Security Checklist that D2SI inspectors will utilize during all Operation Inspections (last two pages of the enclosed Security Program). Any security information obtained by FERC will be treated with the utmost care, and the data will be protected to prevent it from gaining public access. Refer to the enclosed guidance (section 4.22) for details.

The important details pertaining to your responsibilities in the Security Program are summarized here for your information. Licensees/exemptees will be responsible for:

1. 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.
2. Having a single point of contact to FERC for all security related information.
3. Ensuring that security measures do not conflict with License requirements.
4. Ensuring that the actions contained in the EAP, Security Plan, and Recovery Plan are integrated for their projects, if the project has those documents.
5. Communicating to D2SI and nearby dam owners regarding security breaches or incidents, if not expressly restricted by law enforcement agencies.

In addition, licensees/exemptees are required to have in place the following based upon the Security Group classification of their dams (see below for more details about the security grouping):

<u>Security Group 1 Dams</u>
1. Vulnerability Assessment by September 30, 2003
2. Security Assessment by September 30, 2003
3. Security Plan by September 30, 2003
4. Ensure that (current and revised) security and emergency action procedures are integrated

<u>Security Group 2 Dams</u>
1. Vulnerability Assessment not required, but is encouraged
2. Security Assessment by September 30, 2003
3. Security Plan by September 30, 2003
4. Ensure that (current and revised) security and emergency action procedures are integrated

<u>Security Group 3 Dams</u>
1. Security Assessment not required, but is encouraged
2. Security Plan not required, but is encouraged
3. Integration of security and emergency action procedures not required, but are encouraged

If any of your dams are in Security Groups 1 and/or 2, staff from our office will contact you by telephone during the week of June 17, 2002 to confirm the Security Grouping classification of those dams. If all of your dams are in Security Group 3 only, you will not be contacted. (If you wish to confirm Group 3 status only, please feel free to call our office after the week of June 24, 2002. As envisioned, the level of detail required for Vulnerability Assessments, Security Assessments, and Security Plans is highly dependent on the complexity of your hydropower facilities and personnel assets. Instead of requiring specific methodologies, or their equivalent, the scope of these documents should be decided by you, with our guidance if requested. Please refer to section 2 ("Selected Definitions") and section 6 ("Vulnerability Assessments") of the enclosed guidance for additional information.

Our office will offer an opportunity for licensees/exemptees to come in and discuss the Security Program in greater detail. This meeting will also provide you with the opportunity to discuss the Security Groupings of your dams. Attendance is not required, but you are very welcome to come. The meeting for our FERC region has been scheduled for July 23, 2002 from 10AM to 12 Noon . Please contact us by July 8, 2002 if you wish to attend. If the response is overwhelming, meeting space will be filled on a first-requested basis and other meeting dates will be made available. Periodically, we will offer additional meeting opportunities to discuss security as the need arises. Of special note, we hope to hold a workshop next spring in conjunction with the USSD meeting in Charleston, SC to discuss security and emergency preparedness. Please refer to the FERC web page (www.ferc.gov) as information on this workshop, and other meetings, develop.

It is unfortunate that we find ourselves in a situation where infrastructure security must be addressed due to potential terrorists threats. We realize that your response to terrorism must be tailored to your specific needs, and we fully expect that the FERC Security Program will allow us to accomplish that goal. Our intent is to work cooperatively with you to address these potential threats. If you have any questions, please contact Charles Goggins at 212-273-5910 .

Sincerely,

Anton J. Sidoti
Regional Engineer

Enclosure
FERC Security Program for Hydropower Projects, Version 1 (6/4/2002)

FERC Security Program for Hydropower Projects
Version 1 (6/4/2002)

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.
- $ FERC personnel attended a RAM-D Vulnerability Assessment of USACE-Baltimore District project.

Next Steps:

- $ During the FY2002 operation inspections, 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.
- $ Train Key HQ and RO Staff in RAM-D Vulnerability Assessment methodology.

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 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:

Integration of plans - In this program, "integration" of plans is defined as ensuring that there is a 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 understands 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 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 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. 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 Vulnerability Assessment.

Security Plan - A document characterizing 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) identifies the "weak points" or vulnerable project features at a facility. It can also assess 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, information received from the FBI or other government agencies, as well as the consequences of such an attack.

3.0 Objective

As one of the special focuses of the Operation Inspections, by the end of the FY 2002 inspection season, Dam Safety staff will complete inspections to determine if reasonable security measures are in place at all High and Significant Hazard Potential dams. Once reasonable measures are in place, 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. Dam Safety personnel will assist licensees/exemptees when requested, or provide points of contacts to those requesting further information. 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. 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 FERC receives comments from licensees/exemptees, the program can be adjusted as necessary. As we all gain experience with these issues 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 Dam Safety Staff Responsibilities

Dam Safety 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 Dam Safety 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 must be 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.

Dam Safety staff will also review how upgraded security elements impact license articles, especially relating to environmental concerns and recreation. Any closures of required facilities, such as recreational areas, exceeding 30 days may need to proceed through the license amendment process. Permanent closure of such facilities should not be allowed without license amendment.

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. 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 Operation Inspection Documentation and Follow-up

Responses are to be recorded by the 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 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, 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 Dam Safety staff via e-mail. Specific details about the security measures at a facility are not to be recorded by 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 RIMS.

The Operation Inspection Report will include a statement that security has been discussed and reviewed by 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 Dam Safety Staff Review of Security Submissions

In addition to 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. Dam Safety staff should request from the licensee/exemptee an assurance that those additional systems do not conflict with existing license articles or requirements. If there may 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, Dam Safety 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 Dam Safety-HQ.

4.2.4 Dam Safety Staff Training

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 Dam Safety-HQ will be provided as necessary. It is anticipated that annual seminars will be held for 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, 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.
- **$** Having a designated contact to FERC for other security related communications.
- **$** 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 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/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.

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 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 (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 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 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]	Yes[1]	No[2]
Vulnerability Assessment	Yes[1]	No[2]	No
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/developed.

5.0 Threat Alerts and Communications

5.1 Dam Safety 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 Dam Safety-HQ for national consistency. Communication will be handled primarily through the use of email and fax. 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.

Regional Offices will report security incidents to Dam Safety-HQ, who will report, as appropriate, to other 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 Region 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 them.

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 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 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 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 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 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) identifies the "weak points" or vulnerable project features at a facility. It can also assess the potential threat to a facility as based on organizations or people (including locals) who may wish to cause harm to the facility, and may also address the consequences of such an attack. 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 should 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 general, a VA should 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.
- **$** Consequences arising from the implementation of undesirable events.
- **$** 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, 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 Infraguard 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.

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)

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? Days/week (Dam)_____(Pwrhse)_____. Hours/day (Dam)_____(Pwrhse)_____.

4. Are there surveillance cameras? (Dam)_____(Pwrhse)_____(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?_____ 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 for the project? (Group 1 VA required by 9/30/03)_____.

14c. Is there a Security Assessment for the project? (Group 1 or 2 SA required by 9/30/03)_____.

14d. Have security actions been integrated with the 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: Yes_____. 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