# Federal Energy Regulatory Commission

# Division of Dam Safety and Inspections FERC

# Security Program for Hydropower Projects

# Revision 3A

March 30, 2016

Federal Energy Regulatory Commission
Division of Dam Safety and Inspections

**FERC Security Program for Hydropower Projects**

***Revision 3 (Final 8/31/2015)***

## TABLE OF CONTENTS

APPENDICES

# SUMMARY OF CHANGES

Revision 3 is the latest change to the FERC Security Program for Hydropower Projects since it was last revised on 6/3/2009. All changes made from Revision 2 were based on the findings from FERC security field inspections and discussions with industry experts. The following contains a brief discussion of several changes in the Program (minor editorial changes are not identified here):

| PAGE | SECTION | DESCRIPTION OF REVISION 3 CHANGES |
|---|---|---|
| 3 | 3.2 | Licensee/Exemptee Responsibilities now include "both physical and cyber" in the guidance document. |
| 5, 6, 7 | 3.3.1, 3.3.2 & 3.3.3 | A Cyber/SCADA Security Plan must be addressed for all sites with cyber/SCADA concerns (see bullet note 2, page 7, for Group 3 remote control of multiple projects). |
| 6 | 3.3.2 | The Security Assessment for Group 2 Dams must be reprinted at least on a 10 (ten) year cycle, in addition to annual updates. |
| 21 | 4.3 | National Threat Alert System changed from color code system to the National Terrorism Advisory System (NTAS) of Normal, Elevated, and Imminent Alerts. |
| 23 | 5.2 | The Vulnerability Assessment (for a Group 1 Dam) is to follow, at a minimum, the general outline provided in the guidelines. Several suggested topics for the outline of a VA are shown in bold face as required. Effective December 31, 2015. |
| 23 | 5.3 | A "design basis threat" should be chosen to represent the "normal" baseline conditions that the security system is designed against. This can be one of the suggested threat scenarios provided by the FERC, or different, as appropriate. |
| 28 | 6.2 | The Security Assessment (for a Group 2 Dam) is to follow, at a minimum, the general outline provided in the guidelines. Several suggested topics for the outline of a SA are shown in bold face as required. Effective December 31, 2015. |
| 30,31 | 7.2 | The Security Plan for a Group 1 or 2 Dam is to follow, at a minimum, the general outline provided in the guidelines. Several suggested topics for the outline of a SP are shown in bold face as required. Effective December 31, 2015. |
| 36 | 8.0 | Compliance with Section 9.0 Computer Security and SCADA requirements, if applicable, in the Annual Security Compliance Certification Letter. |
| 37-46 | 9.0 | Procedures for Computer Security and SCADA are more detailed and the entire section should be carefully reviewed for new requirements. Effective December 31, 2015. |
| 47 | Appendix A | Cyber questions removed from the FERC Hydro Security Inspection Form 1. |
| 51-55 | Appendix A | A new Cyber Security Inspection Checklist (Form 3) has been added. |
| 56 | Appendix A | New Security Documentation Checklist for a Group 1 Dam. |
| 57 | Appendix A | New Security Documentation Checklist for a Group 2 Dam. |
| 62 – 64 | Appendix C | New Examples of Threat Response Actions for Licensee/Exemptees based on the National Terrorism Advisory System. |
|  | Appendix G | The NERC Security Best Practices list of standards has been removed from this guidance. Refer to http://www.ferc.gov/industries/electric/indus-act/reliability/standards.asp for the latest standards. |

Federal Energy Regulatory Commission
Division of Dam Safety and Inspections

# FERC Security Program for Hydropower Projects

***Revision 3 (Final 8/31/2015)***

## 1.0 PURPOSE

The Division of Dam Safety and Inspections (D2SI) monitors the security programs and measures implemented by dam owners. This document provides guidance to both the FERC licensees/exemptees and staff in the execution of this program. From here forward in this guidance, “licensee” will refer to both “licensees” and “exemptees”.

## 2.0 OBJECTIVE

D2SI conducts periodic security inspections of projects based on the current threat conditions and as determined by the Attorney General and the Office of Homeland Security in order to insure the security of FERC hydropower projects. These inspections determine if the licensees have implemented a security plan appropriate to site conditions and to current threat conditions while remaining flexible enough to address elevated threat conditions. As a special focus of the Dam Safety Inspections, the FERC D2SI Engineer will evaluate the level of security, both physical and cyber, that is in place at facilities having the potential of causing significant to high consequences if attacked (Security Group 1 and Group 2 Dams; refer to sections 3.3.1 and 3.3.2). Additionally, at least a basic level of security is recommended for all lower-potential consequence dams (Security Group 3 Dams; refer to section 3.3.3) and will be reviewed periodically when time and resources are available to D2SI. These security inspections are conducted in conjunction with the Dam Safety Inspections over the inspection scheduling cycle, or as special inspections are required.

## 3.0 REQUIREMENTS AND RESPONSIBILITIES

All Dam Safety Inspections of Security Group 1 and Group 2 Dams include an evaluation of security. These inspections provide an opportunity to review and evaluate the in-place security measures and to monitor and comment on their effectiveness against the current threat conditions that are known to, or perceived by, the licensee. In addition, this guidance provides for a nationally-consistent framework in which FERC dam owners can design and implement their security programs.

### 3.1 General Requirements

Security measures implemented at hydropower facilities are the responsibility of the licensee. D2SI assists licensees when requested, or provides points of contacts to those requesting further information. During the Dam Safety Inspection, D2SI staff monitors actions being taken at FERC dams and comments on these actions specific to the facility. What appear to be deficiencies are discussed with the licensee to arrive at a mutually agreed response.

Recognizing that the current level of threat or warning may result in varying response actions from the licensee, the licensee may need to strengthen the on-site response during heightened threat conditions, whereas at lower threat conditions, relaxation of some security measures may be appropriate. In addition, the FERC recognizes that the overall level of security will vary due to site-specific conditions.

### 3.2 Licensee Responsibilities

Licensees will be responsible for:

- Security at their projects (both physical and cyber); Vulnerability (Risk) and/or Security Assessments of their projects and Security Plans (as appropriate); security upgrades; and communicating with local law enforcement and nearby dam operators.

- Appropriately augment on-site inspections ("walk-downs") of project facilities in light of security; pay special attention to suspicious activities and "danger signs" from vulnerable features or potential failure modes, including visual signs of distress and critical dam safety instrumentation readings; "trigger points" for action arising from critical instrumentation are to be defined.

- Maintain a level of awareness of potential threats to the project in the area and region.

- Provide annual training and information updates to appropriate company employees on security and security plans (physical and cyber), as well as threat; ensure the protection of sensitive information and operational security (OPSEC).

- Designate a primary point of contact to receive FERC security notifications.

- Designate alternate contact(s) to FERC for security related communications, if different from the above contact, which may include 24/7 watch offices, if desired by the owner.

- Ensure that the security contact and dam safety contact for FERC (if they are separate contacts) remain in communication for project responsibilities and operation.

- Involve the responsible security staff/manager, as well as the dam safety/operations manager, in all major security-associated activities for the project site.

- Resolve any security measures that may conflict with License requirements.

- Ensuring the efficient coordination among the procedures contained in various plans, such as the Emergency Action Plan (EAP) and Security Plan(s) (which includes the

Internal Emergency Response and Rapid Recovery) for applicable Security Grouped projects.

- Establish and maintain open communications with FERC D2SI staff and nearby dam operators regarding suspicious activity and security breaches or incidents, if not expressly restricted by law enforcement agencies (refer to section 4.0 for details); notify FERC Regional Office of any suspicious activity/incidents as soon as practical (usually within one working day).[1]

- Having the security contact (or their representative) and all required security documents available for review by FERC D2SI Engineers, especially during the Dam Safety Operation Inspection.

### 3.3 Licensee Requirements

The foundation for the FERC Hydropower Security Program are the three security groups (Security Groups 1, 2, and 3) as based on potential dam hazard classification, project size, potential consequences, and installed generation capacity. Licensees were notified of the security groupings of their dams in a letter sent to them on November 21, 2001, and as reiterated on January 16, 2009. This prioritization effort was based on data that were readily available shortly after the 9/11 attacks.

A reevaluation of the Security Group classifications of FERC dams was undertaken in 2010 by utilizing improved assessment methods that were not available in 2001. Factors used to reclassify the dams were the potential consequences if attacked (C value of the Dam Assessment Matrix for Security and Vulnerability Risk - DAMSVR), the vulnerability of the dam asset (V value), and the Likelihood of Attack against that asset (L value). These Security Grouping modifications were conveyed to licensees in a letter dated January 2010. Dams with a higher potential consequence and vulnerability (as well as being accessible and attractive as a target) were grouped higher than those with lower potential consequences as paired with their vulnerabilities.

**[1] Suspicious Activity Reports (SARs) around the country are being submitted by dam owners to the Dams Sector Portal at DHS through the Homeland Security Information Network (HSIN) computer portal. Participation in this program is voluntary, but highly encouraged so that you can contribute to the state of knowledge regarding SARs across the country and for you to stay informed of similar incidents. To become a member of the HSIN Dams Sector community, please email dams@hq.dhs.gov for a Dams Sector portal access form. As a FERC Licensee, list FERC as your sponsoring agency.**

### 3.3.1 Security Group 1 Dam Requirements

This section provides a brief summary of Security Group 1 Dam requirements. Refer to sections 5.0, 6.0, 7.0, and 8.0 for in-depth requirement details and definitions of terms.

A Security Group 1 Dam is defined by the level of its Consequence, Vulnerability, and Likelihood of Attack values as derived from the DAMSVR (v2) analysis. The definition of what constitutes a Security Group 1 Dam cannot be included in this open document because the level of potential consequences defined for a specified group of dams should not be publically revealed, but can be provided to the licensee during the security inspection. Dams belonging to Security Group 1 will be inspected with a higher level of scrutiny by FERC D2SI. These dams are required to have completed (and have the following security documents on hand during the inspection):

- <u>Vulnerability Assessment</u> (updated annually, and reprinted within the past 5 years).[2] The Vulnerability Assessment for a Group 1 Dam also includes all the details required for a Security Assessment of a Group 2 Dam. A Vulnerability Assessment must also be completed to justify requests for permanent licensed facility closures for any Security Grouped Dam (1, 2, or 3).

- <u>Security Plan(s)</u> (updated as changes are made to security and/or procedures; at least annually). In addition, the Security Plan for a Security Group 1 Dam must be exercised at a minimum of every five years (at least to the Drill level—refer to the FERC Engineering Guidelines, Chapter 6, EAP for details); SP testing may be consolidated into a single test if multiple dams exist within the same watershed and utilize the same responding agencies. The Security Plan must also show how the expected response can be increased as a result of changing threat conditions. The Security Plan must also contain a sub-element (Internal Emergency Response and Rapid Recovery), which shows how security and emergency notification/response actions are integrated and how the project can recover rapidly (refer to section 7.4). The Security Plans(s) must incorporate cyber/ Supervisory Control and Data Acquisition (SCADA) security measures in the plan or develop and maintain a separate cyber/SCADA Security Plan, if used at the site. For purposes of this guidance, cyber considerations apply to remote control/operation of water retaining structures and to the continued operation of Licensed power generation. Issues related to electric reliability and grid stability are covered under different programs.

- <u>Annual Security Compliance Certification Letter</u> (due annually by December 31 and

**[2] Security Group 1 and Group 2 Dams must have all applicable documents available during all inspections and will be monitored during the 2011 Inspection season and beyond.**

submitted to the FERC Regional Engineer). The letter certifies compliance with the Security Group 1 Vulnerability Assessment and Security Plan requirements, highlighting any parameters that have changed from the previous year.

### 3.3.2 Security Group 2 Dam Requirements

This section provides a brief summary of Security Group 2 Dam requirements. Refer to sections 6.0, 7.0, and 8.0 for in-depth requirement details and definitions of terms.

A Security Group 2 Dam is defined by the level of its Consequence, Vulnerability, and Likelihood of Attack values as derived from the DAMSVR (v2) analysis. The definition of what constitutes a Security Group 2 Dam cannot be included in this open document because the level of potential consequences defined for a specified group of dams should not be publically revealed, but can be provided to the licensee during the security inspection. Dams belonging to Security Group 2 will also be inspected by FERC D2SI Engineers at a high level of awareness, consistent with the potential threat level. These dams are required to have completed (and have the following security documents on hand during the inspection):

- Security Assessment (updated annually, and reprinted within the past 10 years).

- Security Plan (updated as changes are made to security and/or procedures; at least annually). The Security Plan must also show how the expected response can be increased due to changing threat conditions; however the changes due to varying threat conditions may not be as stringent as for dams of Security Group 1. The Security Plan must also contain a sub-element (Internal Emergency Response), which shows how security and emergency notification/response actions are integrated; however the Rapid Recovery sub-element is not required for Group 2 Dams. There is no requirement for exercising a Security Plan for a Group 2 Dam, although an exercise program is strongly recommended. The Security Plans(s) must incorporate cyber/Supervisory Control and Data Acquisition (SCADA) security measures in the plan or develop and maintain a separate cyber/SCADA Security Plan, if used at the site. For purposes of this guidance, cyber considerations apply to remote control/operation of water retaining structures and to the continued operation of Licensed power generation. Issues related to electric reliability and grid stability are covered under different programs.

- Requests for Permanent Licensed Facility Closures for any Security Group 2 Dam requires a Vulnerability Assessment to justify the closure (refer to section 3.3.4).

- Annual Security Compliance Certification Letter (due annually by December 31 and submitted to the FERC Regional Engineer). The letter certifies compliance with the Security Group 2 Security Assessment and Security Plan requirements, highlighting any parameters that have changed from the previous year.

### 3.3.3 Security Group 3 Dam Requirements

A Security Group 3 Dam is defined as any FERC dam not meeting the definitions of Security Group 1 or Group 2 Dams. The definition of what constitutes a Security Group 3 Dam cannot be included in this open document because the level of potential consequences defined for a specified group of dams should not be publically revealed, but can be provided to the licensee during the security inspection. Dams belonging to Security Group 3 will be inspected by FERC D2SI Engineers as these dams come up for scheduled Dam Safety Inspections, ranging from 1 to 3 years. There are no security document requirements, however a Security Assessment and Security Plan are highly recommended, and shall be at the discretion of the licensee. Security will be highly dependent upon the opinions of the licensee. FERC comments about Security Group 3 Dams are expected to be minimal.

- Requests for Permanent Licensed Facility Closures for any Security Group 3 Dam requires a Vulnerability Assessment to justify the closure (refer to section 3.3.4).

- Although Security Plan(s) are not required, and only highly recommended, for Group 3 Dams, it should be noted that remotely operated/controlled projects must have appropriate physical and cyber security measures in place to protect cyber/SCADA systems if tied to Group 1 and/or (some) Group 2 dam projects. All Security Groups should consider having cyber security plans if they utilize cyber/SCADA assets. For purposes of this guidance, cyber considerations apply to remote control/operation of water retaining structures and to the continued operation of Licensed power generation. Issues related to electric reliability and grid stability are covered under different programs.

Although some FERC 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 an EAP, and that pertinent contact numbers for law enforcement agencies be placed in the Project’s Contact List.

### 3.3.4 Licensee License and Recreational Responsibilities

Interruptions to recreational and project use due to security concerns are to be minimized to the greatest extent possible. Temporary (30-day or less) restrictions may be appropriate in certain circumstances without prior approval of FERC D2SI, as long as the FERC Regional Office is notified as soon as practical (usually within one working day). Measures affecting recreation and project use in excess of a 30-day duration must be coordinated with the FERC Regional Office prior to implementation.

Requests for permanent facility closures due to security concerns require the completion and sharing 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. The existing Security Group 1 Vulnerability Assessment must be used to justify this request. For a Security Group 2 or 3 Dam, a special (full) Vulnerability Assessment must be completed and used to justify if permanent licensed facility closure is appropriate.

### 3.3.5 Unconstructed Projects

The licensee requirements as described in section 3.3.1 to 3.3.3 (above) for unconstructed projects must be completed no later than 60 days before the initial filling of the project reservoir begins.

### 3.3.6 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 3.3 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.

### 3.3.7 Projects with Dams Not Owned by the Applicant/Licensee

When the applicant/licensee is not the owner of the dam nor is otherwise responsible for the maintenance, operation, and monitoring of the dam, the applicant/licensee is to 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) or Licensee refuses to cooperate with each other, then the appropriate Federal or State Dam Safety Official will be contacted and a meeting moderated by the FERC will be established to resolve the situation.

### 3.3.8 Summary of Security Group Requirements

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

**Table 3.3.8 Security Group Requirements**

| **Requirement** | **Security Group 1** | **Security Group 2** | **Security Group 3** |
|---|---|---|---|
| Security Assessment (SA) | Yes[1] | Yes[1] | No[2] |
| Vulnerability Assessment (VA) | Yes[1,5] | No[2,5] | No[5] |
| Security Plan (SP)[3] | Yes[1] | Yes[1] | No[2] |
| Internal Emergency Response | Yes[4] | Yes[4] | No[2] |
| Rapid Recovery Plan | Yes[4] | No[4] | No[4] |
| Annual Security Compliance Certification Letter | Yes | Yes | No |

**[1] Update requirements: VA – annual update/reprint every 5 years; SP – annual update, or as required; SA – annual update/reprint every 10 years minimum for Group 2 (the SA is included within the VA for a Security Group 1 Dam).**

**[2] Although not required, this item is highly recommended.**

**[3] The SP must address how the licensee is handling the recommended security upgrades identified in either the Vulnerability Assessment and/or Security Assessment, as applied to the site specifically. An SP for a Security Group 1 Dam (and suggested for Group 2 Dams) must be exercised at least every 5 years. At their option, licensees may combine SP testing for multiple projects within the same watershed into one exercise.**

**[4] Internal Emergency Response and Rapid Recovery is a sub-element of the Security Plan and discusses procedures to use to transition between a security incident and the emergency notification/response activities and how to rapidly recover from lost services (refer to section 7.4). Internal Emergency Response and Rapid Recovery is required for Security Group 1 Dams; Internal Emergency Response (only) is required for Security Group 2 Dams.**

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

## 3.4 FERC Responsibilities

### 3.4.1 FERC Security Program Responsibilities

D2SI administers this Program by providing guidance and direction on all matters of security program management. The Regional Engineers are responsible for the execution and implementation of this program within their jurisdiction. Through the use of their engineers, the following is a list (although not all inclusive) of duties necessary to effectively carry out this program:

- Maintain a master list of Security Groupings of Dams under the jurisdiction of D2SI (which will be protected from public view).

- Establish and maintain communications with other federal and state agencies responsible for Dam Safety and Security.

- Participate in the DHS Dams Sector Government Coordinating Council activities and coordinate with the Dams Sector (Private) Coordinating Council. All attempts will be made through these Councils to avoid undue duplication of efforts to the dam sector.

- Contribute to the national database of suspicious incidents at US dams, and pass along pertinent threat information derived from the database to FERC staff and FERC dam owners.

- Maintain positive control of any and all security related FERC memos compiled and developed as a result of this program (refer to section 8.0 for details).

- Provide in-house guidance and training to FERC Engineers.

- Maintain and update this security program periodically to keep current with federal and security best practices within the industry.

- Notify the licensee via letter of their upcoming security inspection and requirements based on the Grouping Categorization of the project. (Note: the letter will indicate that the responsible individual and documents for security at that project be present during the on-site inspection.)

- Conduct meetings and perform an inspection with licensees to discuss/review the security program (both physical and cyber).

- Review, monitor, audit, and evaluate security measures at projects as part of regularly scheduled Dam Safety Inspections (both physical and cyber).

- Review if the actions of the Emergency Action Plan (EAP) and Security Plan for all projects that have those documents are compatible.

- Review all required security documentation as required by the security classification of the dam.

- Where required, become familiar with identified vulnerabilities of the dam.

- Review the thoroughness and periodic security assessments conducted by the licensees as required under the security classification of the dam.

- Facilitate communication on matters of threat alerts and threat information from other federal agencies, nearby licensees, and similar sized projects throughout FERC jurisdiction.

- Complete a Project Security Memorandum, with the FERC-prepared DAMSVR assessment and the Security Checklists (Site and Document) as memo appendices, for Group 1 and 2 Dams.

- Protect information regarding security at projects from public disclosure.

- Review security measures for conflicts with License requirements.

- Coordinate, to the greatest extent possible, FERC security and recreational requirements with NERC security requirements to ensure that the licensee is not subject to conflicting requirements.

### 3.4.2 FERC Engineer Responsibilities for Dam Safety Inspections

The FERC Engineer is the responsible security agent for D2SI on all matters regarding this security program with the licensee representative. During the Dam Safety Inspection, security matters are discussed with the appropriate licensee personnel. The person responsible for security at the facility, or other appropriate personnel, is to be present during these security discussions and inspection. **The letter to the licensee notifying them of the upcoming inspection will clearly state that the security representative attend the security portion of the inspection and have all security documentation with him/her.** Guidance recommendations in conducting security document review and inspections are discussed in the next section.

### 3.4.2.1 Preparation for the Security Portion of the Dam Safety Inspection

The Engineer must be as knowledgeable as possible about the project that will be inspected, and the engineering and dam safety experience of the D2SI Engineers will greatly assist in this need. Prior to the inspection, the following office activities provide solid background material for the inspection (other activities will be needed on a case-by-case basis):

- Review and become familiar with all the technical aspects of the project.

- Review the Potential Failure Modes, keeping in mind how a potential adversary could exploit those vulnerabilities.

- Review the Emergency Action Plan to gain an understanding of the responding agencies involved (including law enforcement) and the potential effects (Consequences) of (whole or partial) dam failure. Consider the effects of discrete feature destruction, such as one or more spillway gates, etc. and how those effects differ from full dam breach consequences.

- Through FERC training, understand how different types of dams and their associated structures can be compromised by various reasonable means (explosive, non-explosive, control-manipulation, etc.)

- Consider how an adversary could gain access from off-site to on-site (land and water).

- Complete (or review an existing) DAMSVR analysis of the project (see section 3.4.3.3 for details).

- Review the previous year’s project FERC Security Checklists (Site and Document) and Project Security Memorandum (comparing the previous year’s data with this year’s data will assist in identifying any changes made in the field).

- Confirm with the licensee that their security representative and security documents will be available for review during the inspection, or at a special meeting.

### 3.4.2.2 Conducting the Security Portion of the Dam Safety Inspection

The Dam Safety Inspection provides the opportunity for the D2SI Engineer to (1) talk to the licensee about their security (physical and cyber), (2) review all security documents (physical and cyber) prepared by the licensee, (3) observe the physical security features, and operational procedures that are used at the site, and (4) record all the observations made during the inspection. This inspection completed by the Engineer will help guide their efforts in evaluating the overall effectiveness of the licensee security plan(s). The following field activities provide solid background material for the inspection (other activities will be needed on a case-by-case basis, and no single list can be all-inclusive):

- Talk to the security representative(s) and the dam operating personnel to obtain a general overview of how the organization views and handles security concerns (physical and cyber). Determine if there is clear instruction and communication between the security representative(s) (Corporate Security) and operational personnel. Determine if roles are clearly established and if everyone "knows what is expected of them" in consideration to security.

- Determine if contact information for responding agencies (police, or other) are clearly posted.

- Determine if operating personnel are aware of all plans and procedures for security, such as how to handle a bomb threat, what activities are permissible for varying levels of threat alerts, etc.

- Determine if operating personnel know what to look for that may be "out of the ordinary". This is often referred to as "suspicious activity", which could include such activities as adversary surveillance, tests of security, illicit intelligence-gathering, and pre-attack rehearsals, etc., which may lead up to an actual attack. (Consider physical and cyber-attack methods.)

- Determine if there is a consistent chain of communication between the field personnel and others within their organization and responding personnel (similar to communications for an EAP).

- Review any required and/or related security documentation. These documents are to include Vulnerability Assessments, Security Assessments, and Security Plans (which includes Internal Emergency Response and Rapid Recovery). (Security documentation requirements are listed in sections 5.0, 6.0, 7.0, and 8.0.) Become familiar with the documents to obtain an understanding of how the licensee security system is designed to work.

- Determine if there are provisions for improving security on a temporary basis for increased levels of threat.

- Review any recommendations that were made in the self-assessment documents (SA, or

VA) and determine the status. Ask for a Plan and Schedule or resolution of outstanding recommendations. Ensure that appropriate recommendations have been implemented and incorporated into the site Security Plan.

- Ensure that all required documents are up to date and (if Group 1) that the Security Plan has been tested within the last five years.

- Confirm your estimations made in the preparatory phase of potential Consequences for the destruction/damage of the dam(s) and appurtenant critical physical structures **(Table 1 of DAMSVR)**.

- Inspect the project to identify all critical physical dam-related assets (features) that are important to the operation of the project. Determine if those assets are vulnerable to a “reasonable worst-case scenario” and determine what consequences would arise from the destruction of those assets. This includes the dam proper and all appurtenant critical physical dam-related structures **(Table 2 of DAMSVR)**.

- Determine how accessible (and visible) the dam(s) and appurtenant critical physical dam-related structures are **(Table 3 of DAMSVR)**.

- Question the licensee about the perceived threat (local, regional, national) **(Table 6 of DAMSVR)**.

- Observe the effectiveness of the security in place as per the current state of threat and the consistency of those observations with the Security Plan guidance **(Table 7 of DAMSVR)**.

- Ensure that the Security Plan(s) include all upgrades to physical, cyber, and operational security (that it is up to date).

- Complete the FERC Security Checklists (Site and Document) as the inspection progresses (a blank copy of the FERC Security Checklists is provided in Appendix A). Further details about the FERC Security Checklists are shown in the next section (3.4.3.2).

- Complete, or verify, the DAMSVR analysis. Using the DAMSVR method prior to the site inspection will facilitate the inspection. Further details about DAMSVR are shown in the next section (3.4.3.3).

- Review upgraded security elements and their impacts on 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 must not proceed without a determination of the need for a license amendment. In addition, requests for permanent facility closures require the completion of a Vulnerability Assessment (even if the dam is classified as a Security Group 2 or 3 Dam) demonstrating how the particular requested closure mitigates a vulnerability that can be exploited. This information will be used to evaluate the current situation and determine the validity of such an action.

Review all your observations with the licensee representatives. If there are no written plans for a Security Group 1 or 2 Dam, request a plan and schedule for their completion and ask the operator how their organization determines and judges the effectiveness of their security response in the interim.

Review all prepared items completed during the inspection, including the Security Checklist and personal observations, and compare observations with the DAMSVR analysis conducted prior/during the site inspection. The Engineer is to review the security program in its entirety with consideration of the level of known threat demonstrated by the licensee. The completed Security Checklist and DAMSVR sheets while in the field must not contain any specifics that could be used to locate and or identify the specific project. (If an electronic file of the Checklist is made outside of the FERC Network, the document is to be scrubbed of any specific names, locations, and descriptions that could identify a specific project/licensee.)

A copy of these completed forms (the Security Checklist and DAMSVR results only) may be provided to the licensee upon request; however the FERC Project Security Memorandum cannot be provided to outside organizations and still remain a decisional (non-public) document (refer to section 3.4.3). The licensee must endeavor to keep the Security Checklist and DAMSVR results secure.

### 3.4.3 FERC Dam Safety Inspection Documentation and Follow-up

#### 3.4.3.1 FERC Project Security Memorandum

The observations and conclusions of the security portion of the Dam Safety Inspection are recorded in the FERC Project Security Memorandum. Included as appendices of the Security Memo are the Security Checklist (see section 3.4.3.2), and the summary of the latest DAMSVR analysis (see section 3.4.3.3). This Security Memo is an internal decisional memorandum, and is considered as Privileged (non-public) working notes that are not submitted to the Commission’s eLibrary system. This memorandum addresses the security posture of the project in generalized terms only, while omitting specific security details. In order to remain as a decisional memorandum, the working copy written from the inspection cannot be shared with the licensee.

A FERC Project Security Memorandum is completed annually for all Security Group 1 Dams and every five years for all Security Group 2 Dams.

### 3.4.3.2 Security Checklists (attached as Appendix 1 of the FERC Project Security Memo)

Observations and responses to security are to be recorded by the FERC Engineer conducting the inspection (using the Security Checklists as a guide) and discussed with the site personnel. As much as possible, comments are fully discussed with the on-site personnel to provide them the opportunity for interactive feedback. Security recommendations made in the field should be of a generic nature. This checklist will help organize thoughts and observations, and is used to capture results of the security inspection. The FERC Hydro Security Checklist is designed in the logical progression of “detect, assess, delay, and respond” while evaluating security. The Security Checklist can provide the framework to ask effective questions in the absence of a written plan and help document observations. The documentation review checklists for Group 1 and 2 dams (see section APPENDIX A) will help identify missing sections of the required SP, VA, SA, and IERRR. The engineer will use this as a guidance to develop additional recommendations for improving the licensee’s security program in order to meet the FERC requirement.

During the inspection, fill out the FERC Hydro Security Checklist and Document Review Checklist in full and provide supporting data in detail for any outstanding concerns or negative checklist responses. New documentation must be entered each time a new security inspection is made (do not utilize the previous forms), although the results from the previous documentation are to be compared to determine if any changes were observed (record any observed changes in detail on a supplemental sheet of the FERC Hydro Security Checklist). All issues identified during the inspection must be discussed in detail on a supplemental sheet of the checklist.

The Checklists must be completed in full during each annual inspection of Security Group 1 and Security Group 2 Dams. When a FERC Project Security Memorandum is completed (see section 3.4.3.1), the checklist is attached as Appendix 1 of the memo. In the off-years for Security Group 2 Dams, it is retained separately in the FERC security files.

### 3.4.3.3 DAMSVR Analysis (summary attached as Appendix 2 of the FERC Project Security Memo)

Completing a DAMSVR analysis allows for the evaluation of the following project and asset values: Consequence (C), Vulnerability (V), Likelihood of Attack (L), Threat (T), and Security System Effectiveness (S). These parameters are then used in the DAMSVR formula to determine comparative risk. The analysis can also be used by FERC Engineers to verify self-assessments that were made by licensees, and also assists Engineers prepare for the security inspection. A DAMSVR analysis of the project (the dam itself and all associated structures) should be completed prior to the inspection of all Group 1 and Group 2 Dams, and will be accomplished according to the following schedule:

- The roll-out date of Version 2 of DAMSVR is 2009, therefore a new DAMSVR analysis for all Security Group 1 and 2 Dams was completed in 2009.

- Every five years thereafter, or

- The first year a new FERC Engineer is assigned to the project, or

- Whenever any of the following substantive changes to the project are made:
  - Physical security
  - Procedural operations (regarding security, personnel, etc.)
  - Cyber/SCADA modifications
  - Addition of new project features, significant project modifications, or changes to downstream conditions
  - Local, regional, or national threat level changes that could affect the project
  - Current Dam Safety Inspection indicates that new information is warranted.

The FERC Engineer must review the existing DAMSVR analysis during the security inspection and should discuss the results of the DAMSVR analysis with the licensee to arrive at mutually-agreed-upon values, if possible. The two main purposes of developing the DAMSVR data are to assist in the proper classification of security groupings and to serve as a cross-check to the Vulnerability and Security Assessments completed by the licensee. When a FERC Project Security Memorandum is completed (see section 3.4.3.1), the Summary Asset Worksheet (SAW) page of the DAMSVR analysis is attached as Appendix 2 of the memo. The entire DAMSVR analysis for all Group 1 and 2 Dams are retained separately in the FERC security files.

### 3.4.3.4 Requests for Additional Security Information

Any requests for additional details regarding security or procedures must not become part of the Dam Safety Inspection Report. Rather, instruct the dam owner that the requested data are needed and that a follow-on telephone request will be made. Record <u>all details</u> about the request in Question 24 of the Checklist (and on the supplemental sheet, if additional space is necessary). Provide a deadline of 30 days from the date of the inspection for a plan and schedule to accomplish the recommendations. The telephone request should be made within five working days of the inspection. The dam owner is to be instructed to provide the information directly to the FERC Regional Office via hand delivery, certified mail, or parcel services, and is to be forwarded to D2SI-HQ via UPS. Such submittals to the FERC are not to be submitted to eLibrary. Even so, the licensee should refrain from including detailed security data within the submittal to the greatest extent possible. All data supplied by the dam owner in this fashion is to be marked as follows (it is suggested that each page be marked with an automatic footnote):

**“Privileged—Security Sensitive Material.”**

Upon return to the office, the FERC Engineer completes the FERC Project Security Memorandum (if due: annually for Group 1 and five-years for Group 2; see section 3.4.3.1), with the Security Checklists and DAMSVR summary page as appendices. If the memo is not due, then prepare other materials as necessary, such as the annual Checklists or the review of the latest DAMSVR analysis. Each year, discuss the results of the security inspection (observations, Memos, and/or Checklists and DAMSVR data) with the Branch Chief. If recommendations or comments are necessary for a Security Group 1 Dam, FERC Regional Office and HQ will review the FERC recommendations to ensure that national consistency is maintained. Any necessary follow-up actions will be communicated to the licensee via regular mail or telephone and recorded in a telephone memo that will be included with the checklist. If the security measures do not require comment for the level of known threat then the FERC Project Security Memorandum will so be annotated.

Electronic versions of any materials produced by D2SI Engineers containing security matters for a specific project will only be retained on computers connected to the FERC network and will be erased from computer hard drives unconnected to the network immediately after preparation. Any work conducted by computer tied to the Internet outside the FERC office will be completed only through the FERC managed clients. Only two paper copies will be retained (refer to the next paragraph for retention details).

All FERC working notes of all security issues are placed in a project folder and filed in a secure location (locked file or safe) with the Regional Engineer, separate from the general files. An additional copy is stored in the FERC HQ building in Washington, DC in a secured file cabinet. This folder contains the security response correspondence received from the respective licensee, the most recent FERC Project Security Memorandum (and attached Security Checklists/DAMSVR), and any subsequently related correspondence or telephone memos, and pertinent field notes. Specific details about the security measures at a facility are not to be conveyed by the FERC Dam Safety staff via e-mail. Details about the security measures at a facility are not to be recorded by FERC D2SI staff by any means other than by the FERC Project Security Memorandum (and attached Security Checklist/DAMSVR). No copies of FERC-generated data arising from the FERC Security Program will be sent to eLibrary.

The Dam Safety Inspection Report includes a statement that security has been discussed and reviewed by the FERC Engineer. No additional details are provided in the Dam Safety

Inspection Report. Suggested wording for the Dam Safety Inspection Report is as follows:

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

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

### 3.4.4 FERC Engineer 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 Engineer must request from the licensee 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 are to be reviewed on a case-by-case basis. However, a thorough analysis of the request will be made and coordination with the Division of Hydropower Administration and Compliance (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.

### 3.4.5 FERC Engineer Training

FERC D2SI personnel will be trained with state-of-the-art vulnerability assessment/threat assessment/alert technology relating to hydropower facilities. Periodic in-house guidance from DS2I HQ will be provided as necessary. When feasible, annual workshops will be held for the FERC and licensee personnel to discuss the progress of the security program, with individual input from licensees. As part of the learning and information-sharing process, the FERC actively interacts and coordinates with other entities having similar security and dam safety programs, such as the Edison Electric Institute, National Dam Safety Review Board, Association of State Dam Safety Officials, National Hydropower Association, Electric Power Research Institute, US Bureau of Reclamation, Tennessee Valley Authority, US Army Corps of Engineers, DHS Dams Sector Councils, etc.

## 4.0 THREAT NOTIFICATION AND COMMUNICATIONS

### 4.1 FERC Staff Communications

In addition to threat alerts issued by the Department of Homeland Security or the National Infrastructure Coordination Center (NICC), appropriate threat notifications and other security communication matters will be provided to licensees by the Regional Office with guidance from the FERC-HQ for national consistency. Threat information can also be available to those licensees who have valid accounts with the U.S. Department of Homeland Security Information Network (HSIN). Licensees will require approval for vetting within HSIN through their sponsoring agency, which for Licensees is the FERC. Special e-mail groups have been established in each FERC Regional and HQ Office. Communication will be handled primarily through the use of e-mail for those licensees with e-mail addresses, and via fax or telephone for those without e-mail 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 notification. This is currently the best system for contacting all licensees, particularly for those who do not have access to the National Electric Reliability Corporation (NERC) alert, or similar, systems. Threat/suspicious activity notifications will be as specific as possible, and all licensees in the affected area will receive the notification regardless of the security grouping of their facilities. The standard format for the notification is as follows:

*"Please respond back via E-mail reply that you have received this message:*

*Security Threat Notification:*
*The <u>(organization)</u> has issued the following security notice on <u>(date/time)</u>:*

*…message…*

*Considering the information in our letter to you dated November 21, 2001 please take notice of this message 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 notification."*

## 4.2 Licensee Communications

Unless specifically restricted to do so by law enforcement agencies (such as for a Law Enforcement Sensitive ongoing investigation), licensees are to report any suspicious activity or security incidents to their FERC Regional Office. The FERC Regional Office will report those security incidents to DS2I HQ, who will report, as appropriate, to other FERC Regions, other licensees (especially in the immediate area of the incident), and other entities with similar security and dam safety concerns (currently the Homeland Security Information Network (HSIN)). It is critical that national dam sector trend analysis be as all-inclusive as possible. As a result, it is highly recommended that all suspicious activity or incidents be reported to the HSIN Suspicious Activity Reports (SAR) tool, regardless of the apparent insignificance of the activity, where intelligence experts will evaluate the data. Contact dams@hq.dhs.gov to become a member of the HSIN Dams Portal community (Licensees may indicate FERC as their sponsoring agency). If any trends are observed from this reporting, they will be pushed down to our dam owners, as appropriate, using the procedures contained in section 4.1, above. Examples of reportable information (as Suspicious Activity) are shown in Appendix C (i). A sample

Suspicious Activity Reporting Form is shown in Appendix C (ii).

Licensees are to 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 are to be notified as quickly as possible by the licensee to provide a coordinated emergency response and/or to protect other facilities. Dam operators are to inform local law enforcement personnel that security-critical information obtained from one facility is to be passed on to other dam owners in the area, and educate them as to the potential negative implications of not informing upstream or downstream facilities of local emergencies. The licensee is to 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 are to 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. Additional information is contained in section 7.4 (Internal Emergency Response and Rapid Recovery).

### 4.3 National Threat Alerts and Example Licensee Response Actions

On April 26, 2011 the United States Department of Homeland Security issued the National Terrorism Advisory System (NTAS) which replaced the color-coded Homeland Security Advisory System (HSAS). This new system considers three Threat Conditions; Normal Condition, Elevated Condition, and Imminent Condition. An Elevated and an Imminent Threat Alert will only be issued when credible information is available.

Normal Condition – No credible terrorist threats against the United States.

Elevated Threat Alert – Warns of a credible terrorist threat against the United States.

Imminent Threat Alert – Warns of a credible, specific, and impending terrorist threat against the United States.

The response actions listed in Appendix D provides examples to licensees for their consideration to implement as based upon the current Threat Condition. These examples are not meant to supersede any existing procedures contained in specific Project Security Plans, but rather serve as examples of what could be implemented to enhance these plans.

# 5.0 VULNERABILITY ASSESSMENTS

## 5.1 Definition of a Vulnerability Assessment[3]

A Vulnerability Assessment (VA) is a formal document and provides an analysis of the factors that define full Security Risk. This assessment ultimately leads to recommended changes to physical security or operational procedures that will serve to decrease overall risk. Traditional risk analysis is defined as (Impact x Threat x Vulnerability). If Risk Analysis is desired by the licensee, a suggested general comparative risk equation that is currently being used by the FERC is shown below, although any method is acceptable (source: DAMSVR; refer to Appendix E) provided it is fully substantiated:

**Relative Risk = {[C * (V + L + T)] ÷ S} ÷ 300**

**Where,**
**C = Consequence (scale of 1 - 10)**
**V = Vulnerability (scale of 1 - 10)**
**L = Likelihood of Attack (scale of 1 - 10)**
**T = Threat (scale of 1 - 10)**
**S = Security (scale of 10 - 1)**
**and 300 is a scaling factor to normalize to the maximum result.**

Hence, the VA must contain a discussion of the following factors:

- Determine consequences arising from the implementation of undesirable events (C).

- Identify vulnerable facilities and features (assets) of a project (V).

- Identify and assess the potential threats (likelihood of attack and adversary types) (L and T).

- Evaluate the effectiveness of the system to thwart undesired events and adversary types (security system effectiveness) (S).

These factors are discussed in greater detail in section 5.3, below.

**[3] The definition of a Vulnerability Assessment in this guidance leads to a Risk Assessment. However, because of the wide uncertainties involved in defining Threat, and the potential for random human intervention, a "pure" Risk value is extremely difficult to obtain because the Risk value is only as good as the variables input into the equation. Therefore, this analysis will lead more to a function of defining vulnerabilities which implies "relative" or "conditional" Risk.**

### 5.2 General Outline for a Vulnerability Assessment

The format, scope, and details of the VA are to be determined by the licensee, but must be sufficient to address the pertinent vulnerabilities of the project. A suggested general outline for a VA is provided below for guidance, although certain factors are vital to be included in the VA. Those topics that are required are highlighted in bold print in the following list:

- Introduction/Scope/Methodology Used/Assumptions.
- List of Critical Physical Dam-related Assets (dam structures and appurtenant structures).
- **Consequences for each identified asset that is damaged and/or destroyed - Required.**
- **Vulnerability of each identified asset - Required.**
- **Inherent accessibility, visibility (attractiveness) of each identified asset - Required.**
- **Threat climate and range of potential threats each asset may be subjected to, and how each identified asset is vulnerable to those levels of threat under consideration - Required.**
- **Effectiveness of the security system/procedures/response to mitigate identified vulnerabilities and resultant consequences. For Security Group 1 Dams, the Security Assessment is a part of, or integral to, the Vulnerability Assessment - Required.**
- **Risk management decisions - Required.**
- **Recommendations (if necessary) to improve the security posture of the facility, including a Plan and Schedule to address all recommendations - Required.**

### 5.3 Details of the Vulnerability Assessment

A multi-person team approach, consisting of several technical disciplines, the dam operator, and a security expert, has been found to be the best way to complete a VA at a dam. The VA must address four important factors: Consequence, Vulnerability, Threat (and its Likelihood), and Security Effectiveness.

The first factor to address is the consequences of an attack. The consequences of an attack on the facility are to include the potential for loss of life (related to the population at risk), damages that occur downstream (and on-site) of the attack (usually in terms of US dollars), and disruption of the services provided by the facility, such as for power generation, water supply, etc. Consequences are to be considered for failure of the dam and for failure of individual vulnerable project assets, 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. Note that the Consequences resulting from complete dam failure (which are often shown in the EAP for the sunny day and flood condition) will be greater than the Consequences arising from the loss of individual assets, such as the loss of one spillway gate. For security risk, consequences from a dam breach are determined from the sunny day, or normal reservoir pool elevation, case.

The second factor to address is the identification of the "weak points" or vulnerable project features (assets) 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 assets, 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 assets so that a coordinated and comprehensive security system is designed. This also assists planners in determining what is being protected and how well those (critical) physical assets are being protected. It is important to keep in mind that an asset may be vulnerable to a certain level of potential threat, but not vulnerable to a lesser-level threat.

A third 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 are to be considered to determine if a successful attack is actually feasible. The advantage of assessing the likelihood of attack is that the amount of resources needing to be committed may possibly be diminished if the threat is really not present, or that less detailed security enhancements may be appropriate if the threat is not as sophisticated. When assessing threat, a history of security/criminal/vandalism incidents specific to the site, and information received from the FBI or other law enforcement agencies specific to the area, is essential. It should be noted that threat needs to be evaluated first on its presence, and if present or suspected, on the groups' capability to successfully exploit a known vulnerability. A good assessment of threat is helpful in that the planner can then determine to what level an asset must be protected against. The threat assessment portion of the VA must be annually reviewed, and updated as necessary, as part of the annual VA update (refer to section 5.4).

The fourth factor to consider evaluates the effectiveness of the site security system against the anticipated adversary attack scenarios. This subcomponent of the VA comprises the 'Security Assessment' requirement for Security Group 2 Dams. This helps to determine if the current security system provides adequate protection and/or warning. The following security items are to 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 are to be made as a function of the overall risk arising from the attack. These recommendations are to be implemented and incorporated into the Security Plan (refer to section 7.0). The recommendations to security enhancement must be made within the VA, with the dam owner preparing a plan and schedule to address all listed recommendations.

Hence, the VA results in a matrix of paired variables, with specific consequences aligned with specific vulnerabilities, resulting from specific threats, as measured against specific security features. Note that each variable will change as other variables are adjusted. These above factors are to be addressed with a fair degree of confidence, with some supportive documentation to substantiate the assumptions. The VA is beneficial in that the existing security can be compared to an assumed 'baseline' threat, where the implications of experiencing various magnitudes of potential threat can be accurately assessed. At a minimum, the licensee must evaluate their on-site conditions against the following levels of threat (this does not imply that such a level of threat is present, but rather provides a wide spectrum to which the security effectiveness can be measured); site-specific threats should always also be evaluated:

- Insider.
- Vandalism/Theft.
- Group of 3-5 individuals with small arms and backpack explosives.
- Group of 3-5 individuals with small arms, vehicles (land and water), and VBIED (delivery/water truck size, and the equivalent for a water-side (boat) attack).
- SCADA controls attack.
- Any identified local/regional/national/transnational threat groups that are appropriate to the site.

It should be noted that the dam owner does not necessarily concede that a certain threat scenario is anticipated to occur, is feasible for the site conditions, or that the dam owner can successfully protect against such a scenario if it is evaluated for purposes of this assessment. In most cases the dam owner relies on a responding agency, such as local law enforcement, to respond to the adversary. As long as the incident is properly reported to the responding agency, it is irrelevant what caused it. The cause will be discovered during the subsequent response or investigation, but the important actions needed to be taken by the dam owner are reporting the incident and recovery. The suggested threat scenarios (above) simply allow the existing security system and procedures to be compared to a wide spectrum of possibilities so that informed decisions can be considered in a changing threat environment and to educate the dam owner as to what would result if that level of threat were applied against them. This is why multiple threat scenarios should be reviewed and considered for evaluation in the VA. It also informs the dam owner about potential deficiencies if future threat levels were to increase, and how to temporarily address increased threat postures. The dam owner is allowed, if desired, to footnote any evaluated scenario with a clause such as "… there is no present evidence to indicate that this level of threat exists in this area …."

The dam owner is to choose a level of threat that is used for "normal" conditions (it can be one of the above scenarios or a different level, if desired) which is often termed the "design basis threat" for the project. This threat level should be applied to the security system to determine "baseline" security effectiveness. If the threat level increases, then security posture/ procedures/operations should be enhanced on a temporary basis as discussed in Section 4.3 and Appendix D.

A good standard to measure security against is provided in the For Official Use Only publication, "Dams Sector Protective Measures Handbook - A guide for Owners and Operators". This document was prepared under the auspices of the U.S. Department of Homeland Security and is available on the Homeland Security Information Network (HSIN) Dams Portal. For additional distribution information and access requiremmailto:ents for HSIN, contact dams@hq.dhs.gov.

## 5.4 Vulnerability Assessment Documentation

All assumptions must be well documented within the VA, including estimates of essential factors (consequences, vulnerabilities, threat, and security). Recommendations (suggested changes to site security) arising from the study must also be clearly defined within the document. A VA must specifically address each Group 1 Dam and must be reprinted (redone) on a five year cycle, beginning on December 31, 2010. In addition to the five-year reprint cycle, each VA must be updated annually, with changes to parameters and conclusions highlighted from the previous year. Any changes or modification can be inserted to the existing VA as attachments. In particular, variations in threat level must be addressed in the update as well as changes arising from on-site modifications to security systems/procedures (which may affect security effectiveness) or downstream conditions (which may affect consequences). Hence, a new threat analysis must be completed annually as part of the annual VA update and should be coordinated through local law enforcement agencies. In this way, the dam owner can verify that the VA has been reviewed and assessed based on the current known threats. If there have been no changes from the previous year, an acceptable update can be a one-page and dated insert to the VA indicating that you have "reviewed the VA and there are no changes" to ensure that it is current. If so, the agency contacted to verify the annual Threat Analysis (and date of meeting or contact) must be shown on the insert.

The annual VA update and 5-year reprint is required whether as a result of being a Security Group 1 Dam, or as a result of a proposed modification to the license requirements of a Security Group 1, 2 or 3 Dam.

<u>A VA must be completed for all Security Group 1 Dams. A VA is also required for any dams where there is a request to permanently (in excess of 30 days) close permanent recreational or other licensed facilities (e.g., recreation or roads) within project lands for security reasons</u>. A Vulnerability Assessment is suggested for all dams, regardless of Security Grouping, as it greatly assists in evaluating the effectiveness of security for site-specific conditions using a risk-based approach. The Security Assessment (refer to section 6.0) must be incorporated within, and as part of, a detailed VA.

Licensees do not submit their VA to the FERC; however they must make the document available for review during each Dam Safety Inspection (exceptions to this request will not be entertained). In lieu of document submittal to the FERC, licensees must submit an annual letter to their FERC Regional Office by December 31 of each year, certifying compliance with the requirements for Vulnerability Assessments of their Group 1 Dams (refer to section 8.0). For licensees with multiple dams, a single annual letter may include detailed compliance certification for all their VA, SA, and SP security requirements, as appropriate.

## 6.0 SECURITY ASSESSMENTS

### 6.1 Definition of a Security Assessment

A Security Assessment (SA) is a formal document and is an abbreviated evaluation of the security procedures and features at the dam without fully accounting for attack Consequences, Vulnerabilities, or Threat. Hence, although the VA fully evaluates the four factors discussed in section 5.0, above (C, V, T, and S), the SA - as the name implies - only addresses an evaluation of Security. For this reason, a full risk assessment cannot be made from an SA alone.

The Security Assessment is discussed in greater detail in section 6.3, below.

### 6.2 General Outline for a Security Assessment

The format, scope, and details of the SA are to be determined by the licensee, but must be sufficient to address the current state of security for the project. A suggested general outline for a VA is provided below for guidance, although certain factors are vital to be included in the SA.

Those topics that are required are highlighted in bold print in the following list:

- Introduction/Scope/Methodology Used/Assumptions.

- List of Critical Physical Dam-related Assets (dam structures and appurtenant structures).

- Inherent accessibility and visibility of each identified asset.

- **Effectiveness of the security system/procedures/response to address anticipated adversaries; always consider known local adversaries, but at a minimum consider how a "generic" intruder (on foot) with no specialized tools, equipment, or weapons could gain access to all identified assets. – Required.**

- **Recommendations (if necessary) to improve the security posture of the facility, including a Plan and Schedule to address all recommendations. – Required.**

### 6.3 Details of the Security Assessment

A Security Assessment must be completed for all Security Group 2 Dams, and is an integral part of the VA of a Security Group 1 Dam. The Security Assessment (SA) is an evaluation of the current state and appropriateness of the on-site security system/procedures 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 identifies if any security enhancements are needed, and specifically what those enhancements consist of. The SA must also address the state of maintenance and readiness of the existing security systems/procedures. The recommendations made from the Security Assessment lead to improved security measures and are to be incorporated into the Security Plan (refer to section 7.0). The recommendations to security enhancement must be made within the SA, with the dam owner preparing a plan and schedule to address all listed recommendations.

The level of response is highly dependent upon several factors, such as site-specific characteristics of the project, and ideally should consider 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 (refer to section 5.0, above) greatly assist with the proper evaluation of site security, and often lead to a more-informed security assessment decision. Without knowledge of the factors evaluated in a full 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. 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 threat it is to be protected 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 in more generalized terms (in a vacuum). The only advantage of completing an SA instead of the more detailed VA is that the SA can potentially be completed with fewer resources and at a reduced effort. By definition, though, the anticipated risk from an incident occurring at a Security Group 2 Dam is significantly less severe than for a Security Group 1 Dam, and thus the level of evaluation detail is not as stringent. Thus, although completion of a VA is encouraged to produce a more-informed decision-making process, the SA does not need to address specific Consequences, Vulnerabilities, or levels of Threat. A Security Assessment is a stand-alone document or can be incorporated within a more detailed Vulnerability Assessment.

Although the SA does not need to fully evaluate Threat - as does a full VA - a security system cannot be evaluated unless it is measured against some level of threat. As a result and for consistency across FERC dams, the SA for a Group 2 Dam must (at a minimum) measure security against a “generic” intruder (on foot) with no specialized tools, equipment, or weapons. However, the licensee should always evaluate to the largest perceived threat pertinent to their facility, if it is known or suspected. This would lead to what is generally defined as the “design basis threat”.

### 6.4 Security Assessment Documentation

All assumptions must be well documented within the SA. Recommendations (suggested changes to site security) arising from the study must also be clearly defined within the document. An SA must specifically address each Group 2 Dam and must be re-evaluated and reprinted (redone) ten years from the most current by December 31, 2010, and reprinted on a ten year schedule. In addition, each SA must be updated annually, with changes to parameters and conclusions highlighted from the previous year. Any changes or modification can be inserted to the existing SA as attachments. In particular, variations arising from on-site modifications to security systems/procedures must be addressed. If there have been no changes from the previous year, an acceptable update can be a one-page and dated insert to the SA indicating that you have “reviewed the SA and there are no changes” to ensure that it is current.

Licensees do not submit their SA to the FERC; however they must make the document available for review during each Dam Safety Inspection (exceptions to this request will not be entertained). In lieu of document submittal to the FERC, licensees must submit an annual letter to their FERC Regional Office by December 31 of each year, certifying compliance with the requirements for Security Assessments of their Group 2 Dams (refer to section 8.0). For licensees with multiple dams, a single annual letter may include detailed compliance certification for all their VA, SA, and SP requirements, as appropriate.

# 7.0 SECURITY PLANS

## 7.1 Definition of a Security Plan

A Security Plan (SP) is a formal document (or set of documents) and constitutes the "Standard Operating Procedures" for the operation of all security concerns (physical, cyber, and procedural) at the dam and the project. The plan may be a single document, or a collection of individual plans that address divergent aspects of security management. In any event, the Security Plan must be comprehensive and usable to the security personnel and also to the operators at the dam. The operators at the dam are often the "eyes and ears" of security and must be aware of, and able to initiate reactions to, security concerns.

The Security Plan is discussed in greater detail in section 7.3, below.

## 7.2 General Outline for a Security Plan

The format, scope, and details of the SP are to be determined by the licensee, but must be sufficient to address the current state of security for the project. As stated above, the Security Plan may be one individual plan, or an organized collection of plans that address different security needs. Licensees are allowed to cross-reference and rely on single sources of information, rather than having to duplicate contents in different plans, as long as the indexing between plans is fairly straightforward. (Hereafter, this item will be referred to as the "Security Plan", whether it is one comprehensive document or an organized collection of plans.) A suggested general outline for a SP is provided below for guidance, although certain factors are vital to be included in the SP. Those topics that are required are highlighted in bold print in the following list:

- Lists of Restricted Areas.

- Lists of Critical Physical Dam-related Assets.

- Physical Security Description/Layout/Inventory.

- **Security Operational Procedures (employee duties/education/document control). – Required.**

- Procedures to address site access (employees and visitors).

- **Key Control Procedures. – Required.**

- Procedures for Civil Disturbance (such as coordination with on-site protests, etc.).

- Response to Bomb Threats.

- Procedures for Temporary Project Closure.

- **Threat Level Contingency Planning (actions to adjust security posture rapidly). – Required.**

- **Communication Procedures and Redundancies. – Required.**

- **Information Technology/SCADA. – Required, if applicable.**

- Security Maintenance, Testing, and Resource (Operation and Maintenance).

- **Internal Emergency Response and Rapid Recovery (coordination with the Emergency Action Plan; see section 7.4, below, for details). – Required, as based on Security Group.**

- **Upgrades and additions to physical and operational security procedures. – Required.**

### 7.3 Details of the Security Plan

A *site-specific* Security Plan is a formal document, and must be available to the dam operator at the site, for all Security Group 1 and 2 Dams. Security Plans are to be kept on-site either in a hard copy or secured electronic form. The one exception to the on-site requirement is for un-staffed dams operated at a central facility, such as a Control Center. In those cases, rather than keeping a Security Plan at a facility without staff present, the Plan may be retained at the control center where the roving operator works. The dam owner may offer reviews of the SP to designated representatives of outside agencies with a “need-to-know”, but at no time should hard copies of the site SP be requested or retained by any outside agency or non-owner. The SP documentation includes a description of security hardware and operational procedures to security concerns at a project or facility. The SP includes 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, as well as procedures to follow and personnel roles and responsibilities. The complexity of the SP is dependent on the specifics of the site and the potential threats to the facility. It should incorporate pre-planned changes to security that can be implemented rapidly for increasing or decreasing levels of threat. A separate Security Plan must be developed for each dam in an owner’s inventory to reflect the specific concerns at each site. The Security Plan is the “operating manual” that is used to manage security specific to each site (dam).

A licensee will have previously completed detailed studies (VA or SA) to evaluate the effectiveness of their on-site security. Any recommendations from those assessments that have been implemented must be fully incorporated into the Security Plan. Therefore, the SP must be updated as site changes are made to reflect the most-current conditions and should not be allowed to become outdated. Procedures contained within the Security Plan for a Group 1 Dam must be tested (exercised) at least every five years to prove that the SP is workable and that the appropriate security and operational employees are knowledgeable of its contents. The exercise can be at the drill or higher level (refer to the FERC Engineering Guidelines, Chapter 6, EAP for details) and can be part of the regular Dam Safety Exercise program, if desired. At their option, licensees may also combine SP testing for multiple projects within the same watershed into one exercise. SP exercising for Security Group 2 Dams is not required, but is strongly encouraged.

### 7.4 Internal Emergency Response and Rapid Recovery

**NOTE: This section replaces the concept of "Security Plans or procedures being fully integrated with the project Emergency Action Plan and Recovery Plan" of Revision 1 to the FERC Security Program for Hydropower Projects (previous section 7.0). Because this was a new section (as of Revision 2) requirement to the Security Plan, this sub-element is treated with additional detail in this program guidance. The other sub-elements of the SP, as listed above, are not discussed in detail, but are equally as important.**

The purpose of this sub-element is to strengthen the response for two major activities that the dam industry has noted as being commonly deficient: (1) emergency (security) notification and communication; and, (2) rapid recovery (of essential services). In previous FERC guidance, this concept was equated to "integration with the EAP". This created questions about whether security concerns should be placed in the Emergency Action Plan (EAP), which was not the intent. Further discussions with dam owners and regulators led to the conclusion that it would be preferable to include these procedures within the site Security Plan rather than the EAP.

#### 7.4.1 Emergency Notification and Communications during a Security Incident

A critical step that needs to be well-rehearsed and thought-out is the pass-off between learning of a serious security incident and the: (a) notification to the local responding force (law enforcement) that deals with the adversary, and (b) the notification of the emergency response personnel (EMA) having the responsibility of notifying and evacuating the public to get them out of harm's way. Any transition between security management and emergency response will often involve separate departments within an organization and the processes to follow must be well coordinated. This includes actions contained in various plans, including all those from the

Security Plan through the Emergency Action Plan. The problem arises where there may be a disconnection between on-site security forces and personnel responsible for emergency response. Therefore, documentation is needed to link these actions seamlessly.

An Emergency Action Plan (EAP) is 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 the EAP. But the EAP does not include plans or procedures for the law enforcement agencies that are trying to stop an attack or coordinate the efforts in the investigation and resolution of the attack. Unless all actions are preplanned and coordinated, the law enforcement component and the emergency response component may conflict at the worst-possible time. It is also critical that the (law) responding force be notified as quickly as the incident is observed to obtain the best chance of thwarting the attack. The dam owner will find that the Emergency Management Agencies (EMA) will also need to be contacted immediately after the incident is discovered to maximize saving lives downstream of the dam. Hence, the dam owner will need to coordinate two simultaneous actions with agencies having separate goals (law enforcement and emergency management) to get word out efficiently in a timely fashion.

Procedures for <u>Internal Emergency Response are to be included with the Security Plan</u> to ensure that there is continuity between the many company documents that may exist, such as Security Plans, COOP Plans, and Emergency Action Plans. Emergency and response actions arising from procedures contained in company documents are to be internally consistent, with few if any procedural conflicts. Authors and administrators of documents within a company are to 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 must be incorporated into an EAP, which would have a wider distribution than a Security Plan. Specifics regarding security protocol or on-site security features are not to be included within the EAP document; however operating personnel must 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. For purposes of document control, it would be preferable not to include Security Plan details within the EAP, but rather to include any pertinent details from the EAP into the project Security Plan (which has tighter document control). The transition from security concern to EAP implementation must be smooth. If the licensee has a dedicated security officer, that person must be made aware of the EAP procedures and must provide comments to the EAP coordinator. This is especially important if any response procedures could conflict with security protocols. All conflicts must be resolved before they surface in an actual situation.

<u>The Internal Emergency Response sub-element of the SP is required for all FERC</u>

Security Group 1 and 2 Dams, and must be updated annually with the SP; especially all contact information with law enforcement agencies.

### 7.4.2 Rapid Recovery of Essential Services

Note: The Rapid Recovery of Essential Services sub-element of the SP is required for all FERC Security Group 1 Dams. Compliance with CIP-009-1 meets the requirements for Recovery of cyber assets (and other NERC Standards related to power generation, if applicable) and need not be repeated through this guidance; however, the Recovery sub-element of the SP should contain a footnote indicating such compliance with CIP-009-1, and others, as appropriate.

One of the effects an adversary may be trying to achieve as a result of an attack is the interruption of essential services, such as power generation, water supply, etc. The Consequences of an attack plays a large role in determining Security Risk, therefore any means of decreasing Consequences will decrease the resulting Risk. As a result, mitigating Consequences is a very cost-effective means of decreasing Risk and improving the overall security response to an attack. There will be a definite benefit to the public (services) and the utility company (economics) if the services that were interrupted at the dam are recovered as quickly as possible.

The Rapid Recovery of Essential Services sub-element of the SP documents the actions an organization takes to recover from a disaster. The disaster can be natural or caused by criminal activity. The Rapid Recovery in this program 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 sub-element is sometimes associated with the Utility Recovery Plan, Continuity of Operation Plan, etc., however those plans are usually at the company level, whereas the Rapid Recovery portion of the SP is intended to bring a specific facility back in operation as efficiently as possible. The Rapid Recovery must 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 also to be considered.

Further discussions about Emergency Action Plans, Recovery Plans, and Continuity Plans, including suggested formats, are included in the DHS publication: “Dams Sector Crisis Management Handbook”, 2008. This document can be downloaded from the Internet at:

http://www.damsafety.org/media/Documents/Security/DamsSectorCrisisManagementHandbook.pdf

A suggested (abbreviated) format for the Internal Emergency Response and Rapid Recovery sub-element of the SP is shown below (refer to the DHS “Dams Sector Crisis Management Handbook” for further details).

- Applicable Emergency Scenarios with Rapid Recovery recommendations
- Incident Command System and Company Internal Assignments/Responsibilities
- Coordination with Local Authorities
- Communications, Maps, and Drawings
- Vehicles, Equipment, Materials and Contractors
- Response Time and Geographical Limitations
- Meals and Lodging
- Internal Maintenance of Plan (including employee training)

A final version from the DHS document regarding Internal Emergency Response and Rapid Recovery planning is also shown in Appendix E.

### 7.5 Security Plan Documentation

All plans, procedures, and hardware relevant to on-site security must be well documented within the SP. An SP must specifically address each Group 1 and 2 Dam and were first required by December 31, 2010. In addition, each SP must be updated annually, with changes to parameters, hardware, and procedures highlighted from the previous year. Any changes or modification can be inserted to the existing SP as attachments or replacements. In particular, variations arising from on-site modifications to security systems/procedures must be addressed. If there have been no changes from the previous year, an acceptable update can be a one-page and dated insert to the SP indicating that you have “reviewed the SP and there are no changes” to ensure that it is current. As stated in 7.4, above, an Internal Emergency Response and Rapid Recovery sub-element must be part of the Security Plan.

Licensees do not submit their SP to the FERC; however they must make the document available for review during each Dam Safety Inspection (exceptions to this request will not be entertained). In lieu of document submittal to the FERC, licensees must submit an annual letter to their FERC Regional Office by December 31 of each year, certifying compliance with the requirements of Security Plans of their Group 1 and 2 Dams, and the exercise status for Group 1 Dams (refer to section 8.0). For licensees with multiple dams, a single annual letter may include detailed compliance certification for all their VA, SA, and SP requirements, as appropriate.

## 8.0 ANNUAL SECURITY COMPLIANCE CERTIFICATION LETTER

Licensees are asked not to submit security documents directly to the FERC due to the uncertainties of interpreting the Freedom of Information Act (FOIA). FERC D2SI believes that security-specific documents can be successfully protected from public release; however it appears that the issue will remain uncertain into the foreseeable future. Specific exemptions to FOIA related to security documents are currently being proposed, but they appear to be far from finalized.

Instead of security document submittal, D2SI Engineers capture necessary details during the Dam Safety Inspection and are recorded only in FERC decisional memos (refer to sections 3.4.3.1 through 3.4.3.4 for details).

In addition, the licensee must submit an annual letter to their FERC Regional Office by December 31 of each year that certifies compliance with all the requirements of the FERC Security Program for Hydropower Projects. To be included in the annual letter is detailed information stating the following (as applicable for the Dam Security Groups):

- Compliance with Vulnerability Assessment (VA) requirements, including reprinting (date of last assessment, which must be within five years of the date of the annual letter).

- Compliance with VA updating for the current year (if not a reprinting year).

- Compliance with Security Assessment (SA) requirements and completion (date).

- Compliance with SA updating for the current year.

- Compliance with Security Plan (SP) requirements and annual updating.

- Compliance with the Internal Emergency Response (Group 1 and 2) and Rapid Recovery (Group 1) sub-element of the SP, with confirmation that all contact information contained within the sub-element has been verified for the current year.

- Compliance with Section 9.0 Computer Security and SCADA requirements, if applicable.

- The last date of Security Plan exercise testing for all Security Group 1 Dams (within five years of the date of the annual letter).

- Confirmation of the primary (and alternate) security contact. Include his/her telephone number, mailing address, and e-mail address. This contact should include the e-mail address that D2SI will use in any future security notices (refer to section 4.1).

Sufficient detail to certify program requirements for each Group 1 and 2 Dam owned by the licensee must be included in the annual letter (all dams owned by a licensee may be included in one letter, if desired); however, security-specific information should not be included in this letter. It is suggested that the letter be signed by the Chief Dam Safety Engineer, Dam Safety Coordinator, or other official contact (such as the FERC compliance representative).

Mark all annual security compliance certification letters as follows:
**"Privileged—Security Sensitive Material."**

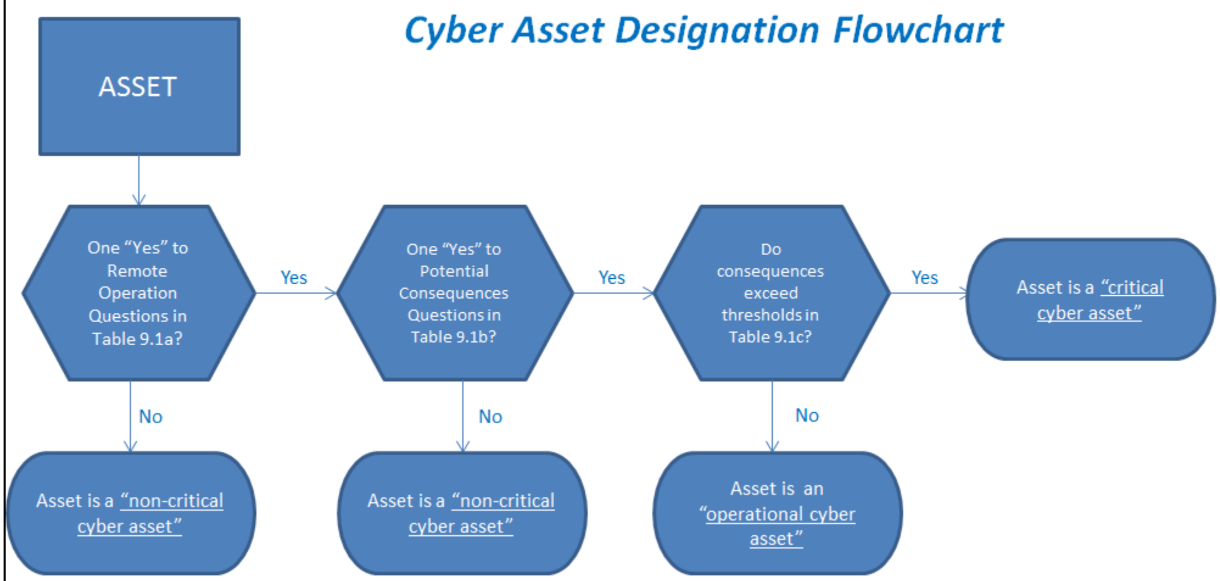
## 9.0 COMPUTER SECURITY AND SCADA

### 9.1 Introduction

**Section 9.0 has been thoroughly revised and will become effective as of January 1, 2016. For purposes of these guidelines only, the emphasis on cyber security and Industrial Control Systems (e.g. SCADA) relates to two main consequences: 1) the unintentional release of all or part of the reservoir (presenting a hazard to downstream populations and infrastructure); and, 2) non-operation of a Licensed facility (loss of significant power generation). Because of this, not all Licensees are required to follow the requirements of Section 9. The flowchart below in Figure 9.1 determines asset criticality and whether the Licensee must follow Section 9. If the asset result is "non-critical" then the Licensee does not need to adhere to Section 9, although voluntary conformance may assist in the strengthening of Licensee business continuity. Details for each step are shown in Section 9.1.1.**

***Note: Only Group 3 dams that are interconnected to operational or critical cyber assets of Group 1 or 2 dams will be subject to Section 9.**

**Figure 9.1: Licensee applicability of Section 9.0.**


Cyber Asset Designation Flowchart
ASSET
One "Yes" to Remote Operation Questions in Table 9.1a?
Yes
One "Yes" to Potential Consequences Questions in Table 9.1b?
Yes
Do consequences exceed thresholds in Table 9.1c?
Yes
Asset is a "critical cyber asset"
No
Asset is a "non-critical cyber asset"
No
Asset is a "non-critical cyber asset"
No
Asset is an "operational cyber asset"

- *"Non-critical cyber asset" must re-evaluate flowchart annually*
- *"Operational cyber asset" must complete Questions 5-33 of the FERC Hydro Cyber/SCADA Checklist and develop baseline cyber security measures*
- *"Critical cyber asset" must complete Questions 5-33 of the FERC Hydro Cyber/SCADA Checklist and develop baseline and enhanced cyber security measures*
- *Any negative response to Questions 5-33 require a plan and schedule to address*

### 9.1.1 Determining if the Facility Falls Under the Requirements of Section 9.0

Every Group 1 and 2 dam will be required to fill out the FERC Hydro Cyber/SCADA Security Checklist, Form 3, Questions 1 – 4 to determine cyber asset designation and discuss this information with the project engineer during the next Operation Inspection.

#### 9.1.1.1 Remote Operation Determination

Responses to the following four questions will determine if the dam under consideration falls under the requirements of Section 9.0 (Computer Security and SCADA) (also refer to Inspection Checklist, Form 3, Questions 1 through 4):

Table 9.1a

| **Project Name:** | | |
|---|---|---|
| **REMOTE OPERATION DETERMINATION** | **YES** | **NO** |
| 1. Does the facility/project utilize automated or remote (off-site) control of data acquisition, such as critical instrumentation or operation data? | | |
| 2. Does the facility/project utilize automated or remote control of power generation data or power generation controls? | | |
| 3. Does the facility/project utilize automated or remote control of water management data or direct control of water retention features? | | |
| 4. Is there an interconnection of computer Systems from/to this facility/project to other dam(s)? | | |
| o **Note:** If there is a virtual (System) interconnection to other facilities that falls under Section 9.0 of the guidelines, that facility is also inclusive of 9.0. | | |

#### 9.1.1.2 Cyber/SCADA Consequence Determination

If any response from “Remote Operation” (9.1a, above) results in a “Yes”, the licensee will be required to further evaluate the potential consequences of losing that capability (in relation to safe operation of the facility) and/or the unintentional (misoperation) or intentional (insider or external attack scenario) compromise of that remote operation related to Table 9.1b.

Table 9.1b

| **Project Name:** | | |
|---|---|---|
| **Cyber/SCADA Consequence Determination** | **YES** | **NO** |
| 1. Releasing the reservoir, | | |
| 2. Losing power generation, | | |
| 3. Loss of other associated dam/reservoir mission(s) such as navigation, water supply, etc. | | |
| 4. For gate loss and downstream flow considerations, assume all gates are fully open, with no remediation response for 48 hours | | |
| 5. For dam failure potential, consider if cascading actions from operational loss could cause the dam to fail (e.g., similar to the 2009 Sayano–Shushenskaya* hydroelectric power station accident, if taken to dam failure). | | |

*http://www.waterpowermagazine.com/features/featuresayano-shushenskaya-accident-presenting-a-possible-direct-cause/
http://www.powermag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/

If any of the above considerations apply to the project, the dam and all interconnected facilities must follow Section 9.0. To determine criticality of the cyber asset, refer to the following table.

Table 9.1c

| **Follow Section 9.0 (Cyber/SCADA) requirements if any potential Consequence arising from compromise of the Cyber/SCADA System is greater than the following values the asset is critical.**<br>**(Consider Consequences for all potential loss of services (power, water, etc.) and the potential for either full or partial uncontrolled release of the reservoir. Each scenario may generate different Consequence values and should correlate with DAMSVR (or similar methodology) results.)** | | | |
|---|---|---|---|
| **Consequence Description** | **Threshold Value** | **YES** | **NO** |
| The potential Population at Risk (PAR) within 3 miles of dam | > 60 people | | |
| The potential PAR within 60 miles of the dam | > 800 people | | |
| The total PAR due to the reservoir release scenario | > 12,500 people | | |
| Total economic losses (replacement/revenue and D/S damages) | > $300 Million | | |
| Disruption of essential services (power, navigation, water, etc.) | > municipal-wide disruption | **1** | **2,3,4** |

**1.** Powerhouse(s) connected to one cyber asset with installed capacity greater than or equal to 1,500 MW are Critical.
**2.** Powerhouse(s) connected to one cyber asset with installed capacity equal or greater than 100 MW but less than 1,500 MW are Operational. **3.** Powerhouse(s) connected to one cyber asset with installed capacity less than 100 MW are Non-critical.
**4.** If a generating unit qualifies as having black start capability, regardless of generating capacity, it is considered Operational.

If any Cyber/SCADA Consequence value is greater than the values in the above table, then this facility is required to implement baseline and enhanced cyber security measures. If the dam must follow Section 9.0, continue with an analysis of responses to Questions 5 through 33 of Inspection Form 3 (Appendix A). Licensees will be asked to implement baseline and enhanced Cyber/SCADA security procedures/measures that result in positive responses to all Form 3 Questions 5 through 33, or to provide a plan and schedule (P&S) as to when this level of protection can be achieved. Acceptance of the P&S is based on C severity.

If any Cyber/SCADA Consequence values are equal to or lower than the values shown in the above table, then the facility is only required to implement baseline cyber security measures under Section 9.0 as well as answers to questions 5 – 33 of the FERC Hydro Cyber/SCADA Security Checklist. Licensees will be asked to implement baseline Cyber/SCADA security procedures/measures that result in positive responses to all Form 3 Questions 5 through 33, or to provide a plan and schedule (P&S) as to when this level of protection can be achieved.

**Note: Interconnected Group 3 dams will be required to develop the same level of protection (baseline or baseline/enhanced measures) depending on the Group 1 or 2 dam's cyber asset criticality.**

#### 9.1.1.3 Summary of Licensee Responsibilities

- Non-Critical Cyber Assets
  - ***re-evaluate cyber assets annually***
- Operational Cyber Assets*
  - ***must complete Questions 5 – 33 of the FERC Hydro Cyber/SCADA Checklist***
  - ***provide a plan and schedule to all negative responses***
  - ***develop baseline cybersecurity measures.***
- Critical Cyber Assets*
  - ***must complete Questions 5 – 33 of the FERC Hydro Cyber/SCADA Checklist***
  - ***provide a plan and schedule to all negative responses***
  - ***develop baseline and enhanced cybersecurity measures.***

***All interconnected facilities also apply.**

#### 9.1.1.4 Definitions

The control systems used by operators to manage their projects are vital to the project's safe and efficient operation. The growing convergence of information technology (IT) and control systems brings with it increased capabilities, but also increased exposure to cyber-attacks against projects. Developing and implementing appropriate security measures reduces the risk to control systems. In the case of legacy components with few or no security features, compensatory controls should be applied as part of an overall defense-in-depth approach.

In this section, the following definitions apply:

- System: Refers to interconnected hardware and software components comprising computers, databases, applications, and control monitoring devices that together perform a particular function or interrelated set of functions.

- Control Systems: Refers to Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

- Supervisory Control and Data Acquisition (SCADA) System: Refers to a specialized computer system which includes sensors for gathering and analyzing real time data regarding operation of hydroelectric generation and water management systems. A SCADA system gathers information, such as how much electricity a generator is producing, transfers the information back to a central location, alerting the operators if abnormal conditions are occurring, carrying out necessary analysis and control, such as determining if abnormal conditions are critical, and displaying the information in a logical and organized fashion. Sometimes, these systems are called Process Control Systems (PCS) and Distributed Control Systems (DCS). Reference: NIST SP 800-82, Sections 2.1 and 2.4. For this guidance, SCADA also refers to remote operation of water retention features, such as spillway gates, penstocks, etc.

- Cyber Asset: Refers to an individual computerized system that performs operational tasks at hydroelectric and water management facilities.

## 9.2 Critical Cyber Asset Identification

After critical and operational cyber assets are determined (Figure 9.1), the licensee must develop and maintain an accurate inventory of its cyber assets and cyber systems. When it is more convenient to classify the criticality of cyber assets as a group then they can be classified as a “cyber system”.

Owners/operators should evaluate cyber assets and classify them using the following criteria:

- Critical Cyber Asset or Critical Cyber Systems: Refers to those that are essential to the safety and/or objectives of the project that exceed the consequence threshold.

- Operational Cyber Asset or Operational Cyber Systems: Refers to those that are essential to the safety and/or objectives of the project however, does not exceed the consequence threshold for critical cyber assets.

- Non-Critical Cyber Assets or non-critical cyber systems: Refers to those systems that are isolated from remote monitoring and controls.

## 9.3 Security Measures for Cyber Assets

The two tables below show the baseline and enhanced cyber security measures (with NIST References) that project operators should apply to cyber assets to reduce the risk to control systems.

| **Table 9.3a BASELINE CYBER SECURITY MEASURES**<br>**The baseline measures should be applied to all cyber assets or cyber systems** | |
|---|---|
| **General** | Provide physical security and access controls to cyber assets. Ref: NIST SP 800-82 Section 6.2.1. |
| | Monitor and periodically review (not to exceed 18 months) network connections, including remote and third-party connections. |
| | Evaluate and reassess the role of wireless networking for risk before implementation. Ref: NIST SP 800-153. |
| | Review and reassess all cyber security procedures annually. Update procedures as necessary. |
| | Review and reassess cyber asset criticality periodically, (not to exceed 12 months). In addition, criticality should be determined as all new cyber assets are added to the environment. |
| **Information Security Coordination and Responsibilities** | Develop a cross-functional cyber security team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. Ref: NIST SP 800-82 Section 4.2. |
| | Define information and cyber security roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors. |
| | Establish and document standards for cyber security controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle. Ref: NIST SP 800-82 Section 6.2.15, NIST SP 800-23, NIST SP 800-36, NIST SP 800-64 and DHS Cyber Security Procurement Language for Control Systems. |
| **System Lifecycle** | Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the SCADA control system architecture is critical for the creation of a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software. Ref: NIST SP 800-27, NIST SP 800-64, and NIST SP 800-70. |
| | Establish and document policies, standards, and procedures for assessing and maintaining system status and configuration information, for tracking changes made to control systems network, and for patching and upgrading operating systems and applications. Ref: NIST SP 800-40. |

| | |
|---|---|
| | Establish and document policies, standards, and procedures for the secure disposal of equipment and associated media. Ref: NIST SP 800-82 Section 6.2.10 and NIST SP 800-88. |
| **System Restoration and Recovery** | Plan and prepare for the restoration and recovery of control systems in a timely manner as specified in the facility's recovery procedures. Ref: NIST SP 800-82 Section 5.13, NIST SP 800-82 Section 6.2.6, NIST SP 800-34, and NIST SP 800-100. |
| | Review the restoration and recovery plan for control systems including annual testing of plan. |
| **Intrusion Detection and Response** | Establish policies, standards, and procedures for cyber intrusion monitoring, detection, incident handling, and reporting. Ref: NIST SP 800-61, NIST SP 800-82 Section 5.1, NIST SP 800-82 Section 5.16 NIST SP 800-83, NIST SP 800-94 and NIST SP 800-82 Appendix E. |
| **Training** | Provide training in information security awareness, on an annual basis or as necessitated by changes in the control system, for all users of control systems before permitting access to the control systems. Individuals with significant control systems security roles should have advanced training specific to their roles. Ref: NIST SP 800-16, NIST SP 800-82 Section 6.2.2 and NIST SP 800-50. |
| **Access Control and Functional Segregation** | Segregate and protect the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies both to wired and wireless networks. Ref: NIST SP 800-82 Sections 5.2, 5.3, 5.5, and 5.6. |
| | Use control systems servers and desktop computers only for approved control system activities. |
| | Establish and enforce access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks. Ref: NIST SP 800-82 Section 6.2.1 and Ref: NIST SP 800-82 Section 6.2.7. |

**Table 9.3b ENHANCED CYBER SECURITY MEASURES**
**In addition to baseline measures, operators should apply enhanced measures to all cyber assets or cyber systems.**

| | |
|---|---|
| **Access Control** | Restrict physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, passwords, secured communication gateways, access control lists, authenticators, separation of duties practices, least privilege practices, and/or other secure access mechanisms and practices. Ref: NIST SP 800-82 Section 6.2.1 and NIST SP 800-82 Section 6.2.16. |
| | Conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Evaluate the need for enhanced networking control technologies for wireless networks prior to implementation. Ref: NIST SP 800-115 Section 6 and NIST SP 800-82 Section 3. |
| **Vulnerability Assessment** | Conduct periodic vulnerability assessments of the control system security, including as appropriate in a non-production environment, not to exceed 12 months. Ref: NIST SP 800-40 and NIST SP 800-82 Section 6.2.14, NIST SP 800-115 and NIST SP 800-82 Appendix E. |

**http://csrc.nist.gov/publications/PubsSPs.html**
**https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf**

### 9.4 During the FERC Dam Security Inspection

The FERC Hydro Cyber Security Checklist, Form 3, is to be filled out by the Licensee prior to the Operation/Security Inspection and discussed with the FERC Engineer during the inspection. During the Dam Safety Inspections, the FERC Engineer inquires about measures taken by the licensee regarding Industrial Control System (ICS) assets for dam operation, and remote operation of project facilities. The D2SI level of interest does not extend into the corporate business network unless proper cyber security access controls are not implemented between the networks and the business network cannot control any aspect of operations. Discussions also do not include assets related to electric reliability or the reliability of the grid. During the inspection, discussions about cyber security controls will be focused on those remote operations that could impact water retention structures, such as the dam, spillway gates, power released, etc., and those issues affecting power generation. Discussions are to be made to ensure that cyber security plans and measures are in place and proper coordination has been made with authorities, such as the FBI. The FBI maintains an incident database and works with those that depend on cyber controlled systems for operations and coordinates activities and technical needs to protect such systems (also refer to section 4.0, above, regarding communication and notification of security incidents). Cyber systems are to be updated consistent with best security practice, and if currently applicable to the owner, consistent with NERC-CIP requirements.

The FERC Office of Electric Reliability requires certain owners, operators and users of bulk power systems to comply with the North American Electric Reliability Corporation's (NERC), Critical Infrastructure Protection Standards (NERC-CIP). These standards focus on the reliability/transmission of power within the Bulk Electric System (BES) and not the potential downstream impacts (population at risk and economic damages) caused by misoperation/failure of water retention features. However, it is possible that a specific cyber asset may fall under both jurisdictions. In this case, the asset must meet NERC-CIP requirements in order to fulfill D2SI's criteria. The CIP standards being met for the specific cyber asset are to be referenced in the security plan(s) and discussed with the project engineer during the dam safety inspection. If a compliance inspection has been performed, the inspection results, any deficiencies identified, and corrective actions taken should also be available for review during the dam safety inspection in order to confirm compliance to Section 9 and prevent duplication of effort.

Information about the NERC-CIP Standards can be found at the FERC website (www.ferc.gov) at:

http://www.ferc.gov/industries/electric/indus-act/reliability/standards.asp

(End of FERC guidance; Appendices follow.)

## FERC SECURITY CHECKLIST (v5)

| **Field Observations: (Provide detailed supplemental information to the right)** | **Y** | **N** | **NA** | **Comments**<br>**(Provide additional details – especially any "No" answers – here and separate sheets, if necessary. Indicate NA if not appropriate to site.)** |
|---|---|---|---|---|
| **DETECTION AND ASSESSMENT**<br>1. Is the site manned? Dam? | | | | Days/week________Hours/day________. |
| Powerhouse? | | | | Days/week________Hours/day________. |
| 2. Are there surveillance cameras in use? Dam? | | | | |
| Powerhouse? | | | | |
| Other? | | | | |
| How are they viewed/checked? | | | | |
| 3. Is the frequency of walking inspections appropriate (safety and/or security)? | | | | Note the frequency of these inspections: |
| Personnel control/ID badges used? | | | | |
| **DELAY**<br>4. Is the dam site fenced with gates/doors locked (if appropriate to the site)? | | | | |
| 5. Is access restriction to the dam/facilities appropriate and in-place? Foot? | | | | |
| Vehicle? | | | | |
| Boat? | | | | |
| 6. Are spillway/gate controls secured against unauthorized access? | | | | |
| 7. Are powerhouse doors/ windows locked? | | | | |
| Alarms/motion detection/cameras? | | | | Specify details: |

| | | | | |
|---|---|---|---|---|
| Can systems be easily bypassed? | | | | |
| 8. Water conveyance system: Access restricted? | | | | |
| Surveillance? | | | | |
| 9. Is critical performance monitoring equipment secured against tampering? | | | | |
| **Field Observations** | **Y** | **N** | **NA** | **Comments** |
| **RESPONSE**<br>10. Are law enforcement phone numbers posted? | | | | |
| 11. Are there redundant communications? | | | | |
| 12. How long it takes the operator if detected to respond to unauthorized access? | How is detection made? | | | |
| What is that response? | | | | |
| 13. Can law enforcement be quickly notified? | | | | Identify enforcement agenc(ies): & capabilities: |
| Estimated time for arrival? | | | | |
| **INTEGRATION & RISK MANGMT.**<br>14. Describe assessment of threats, vulnerable features and potential impacts. Include switchyards & transmission lines, etc. Also consider elements of operations that could be subject to cyber attack. | Last time consultation with law enforcement was made to determine threat: | | | |
| 15. Steps taken to improve security: Past year: | | | | |
| Long term plans: | | | | |
| 16a. Is there a Security Plan (Group 1 or 2) | | | | If “Yes” is it acceptable?<br>Is there a Response/Recovery Plan component? |
| Are there different site-specific response levels covered in the Security Plan for varying threat? | | | | Summarize levels/activities: |
| Are the measures on the day of inspection consistent with the current threat level? | | | | If “no” explain: |
| 16b. Has Security plan been revised since last field change? | | | | When it was last exercised & what type? |
| 17. Is there a Vulnerability Assessment? (Group 1) | | | | If “Yes” is it compliant? |
| 18. Is there a Security Assessment? (Group 1 or 2) | | | | If “Yes” is it compliant? |
| 19. Are all actions an plans fully integrated? | | | | |
| 20. Do any security measures conflict | | | | |

| | | | |
|---|---|---|---|
| with any license requirements? | | | |
| 21. Is there HAZMAT/fuel storage on-site? | | | Describe: |
| If so, is access secured? | | | |
| 22. Are critical drawings/plans/records secured from unauthorized access? | | | |
| 23. We have no comments about the Security Measures observed: | | | If no comments, check “No”; if comments needed, check “Yes”. |
| If comments needed, follow-up actions will be made and tracked | List potential remediation discussed: | | |

**Project Security Summary Information – Form 2**

| Security Information | Comments<br>(Provide detailed information on separate sheet, if necessary) |
|---|---|
| A. Number of security/surveillance incidents in past year. | Description (indicate if it was it reported to FERC) |
| B. Owner expressed specific security concerns or questions. | |
| C. Number (description) of data requests or site visits by DHS PSA or other assessment groups | |
| D. Changes made to security since last inspection<br>None made: | Indicate “None” by checking here:______.<br>Do previous studies show prior posture was adequate?(y/n)_______. |
| Following changes were made to physical site security: | If so, describe changes: |
| Following changes made to procedural operations (incl. threat level increase additions, employee actions, etc.): | If so, describe changes: |

| | |
|---|---|
| Following changes/additions made to cyber/SCADA operations: | If so, describe changes: |
| Overall Risk to security reduced due to above modifications because of: | (Cite critical pre-modification ASR value(s) and show if modifications decreased the ASR Risk value.) |
| E. A discussion was made with site personnel regarding no security materials submittal, and hard-copy only submittal of annual security compliance certification letter | Yes, discussion was made (check if so):_________.<br>No, discussion was not made (reason why)____________________. |

## FERC Hydro Cyber/SCADA Security Checklist – Form 3

*Modified – January 14, 2016*

| **Field Observations: (Provide detailed supplemental information to the right)** | **Y** | **N** | **NA** | **Comments**<br>**(Provide additional details – especially any "No" answers – here and separate sheets, if necessary. Indicate NA if not appropriate to site.)** |
|---|---|---|---|---|
| **FACILITY Cyber/SCADA CONCERNS**<br>1. Does the facility/project utilize automated or remote (off-site) control of data acquisition, such as critical instrumentation or operation data? | | | | |
| 2. Does the facility/project utilize automated or remote control of power generation data or power generation controls? | | | | |
| 3. Does the facility/project utilize automated or remote control of water management data or direct control of water retention features? | | | | |
| 4. Is there an interconnection of computer Systems from/to this facility/project to other dam(s)? | | | | If you answer "Yes" to any of questions 1, 2, 3, or 4, determine if this dam is subject to Section 9.0 of the Security Guidelines (9.1.1.2). If "yes", continue with questions 5 through 33. If "no", the analysis can stop here. |
| 5. Are other FERC regulated projects controlled by this facility? | | | | If so, which projects? |
| 6. Are physical protection measures in place for the control room/facility? | | | | |
| 7a. Does the facility/project have a separate Cyber/Industrial Control System (e.g. SCADA) Security Plan? | | | | |
| 7b. If not, is Cyber/Industrial Control System (e.g. SCADA) Security included in another plan? | | | | If so, what is the plan? |
| 8a. Does the project have any (hydroelectric) cyber assets which are subject to NERC-CIP Standards? | | | | If so, what is the asset: |
| 8b. If a NERC-CIP compliance audit has been performed, have all identified deficiencies been addressed? | | | | If not, when is this scheduled to be completed? |
| 9a. Have all facility/project Cyber/ICS assets been inventoried/identified? | | | | |

| | | | | |
|---|---|---|---|---|
| 9b. Have the assets been designated as critical, operational, or non-critical? | | | | |
| 10. Does the facility/project have Business Cyber Assets (non-industrial control systems which include corporate email, human resources, company website, etc.)? | | | | |
| 11a. Are the Industrial Control System (e.g. SCADA) and non-Industrial Control System networks segregated and access controls applied to prevent unauthorized communication between these networks? | | | | |
| 11b. Within the Industrial Control System environment (to include building services such as HVAC) are the networks segregated and access controls applied to prevent unauthorized communication between these networks? | | | | |
| 12a. Do any vendors or 3rd parties have remote access to your network? | | | | |
| 12b. If yes, are access controls implemented to prevent and monitor for unauthorized attempts and access to systems and operations? | | | | |
| 12c. If yes, is activity logged and reviewed at least weekly? | | | | |
| 13a. Does the facility/project utilize wireless in the Cyber/SCADA system? | | | | |
| 13b. If yes, are access controls implemented to prevent and monitor for unauthorized attempts and access to systems and operations? | | | | |
| 14a. Are cyber security controls implemented within the ICS network that allow for logging, monitoring, detection, and isolation of an anomalous cyber event? | | | | |
| 14b. Is there a dedicated team to review the information? | | | | |
| 14c. How often does the review occur? | | | | |
| 15. Is a configuration and patch management program established for both ICS and non-ICS networks? | | | | |
| 16. Does a back-up site exist and are systems routinely backed-up for ICS and non-ICS networks? | | | | If yes, how often are back-ups tested? |

| | | | | |
|---|---|---|---|---|
| 17. Do you have a policy to address removable and portable media? | | | | |
| 18a. With respect to Tables 9.3a of the Security Guidance, are “General” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18b. Are “Information Security Coordination & Responsibilities” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18c. Are “System Lifecycle” baseline cyber security measures being implemented | | | | If no, state expected completion date and itemize as necessary. |
| 18d. Are “System Restoration & Recovery” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18e. Are “Intrusion Detection & Response” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18f. Are “Training” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18g. With respect to the tables in Section 9.3a, are “Access Control & Functional Segregation” baseline cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18h. With respect to Tables 9.3b of the Security Guidance, are “Access Control” enhanced cyber security measures being implemented? | | | | If no, state expected completion date and itemize as necessary. |
| 18i. Are “Vulnerability Assessment” enhanced cyber security measures being implemented? | | | | If no and required, state expected completion date and itemize as necessary. |
| **SYSTEMS AND ASSETS**<br>19a. Do you maintain an inventory of your technology systems, software, and assets? | | | | If yes, how often is this redone? |
| 19b. Is operational data/configurations removed from systems before they are decommissioned? | | | | |
| 20. Have you identified the systems, assets, information, and processes that are essential to your organizational mission? | | | | If yes, how often are they reviewed? |
| 21. Do you have appropriate access control policies and procedures in place for all systems and assets with particular focus on those that are critical? | | | | If yes, how often are they reviewed? |

| | | | | |
|---|---|---|---|---|
| 22. Are your critical systems and assets appropriately separated or secured from your non-critical systems and assets? | | | | |
| **RESOURCES**<br>23a. Do you assess the threats to your organization and the resources available for an appropriate defense? | | | | If yes, how often are they reviewed? |
| 23b. Do you perform this assessment independently? | | | | If no, state vendor/consultant/other 3rd party: |
| 24a. Do you assess the resources available to govern and implement your security strategy? | | | | If yes, how often are they reviewed? |
| 24b. Do you perform this assessment independently? | | | | If no, state vendor/consultant/other 3rd party: |
| **INCIDENT RESPONSE**<br>25a. Do you maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events (and their physical protection)? | | | | |
| 25b. Do these include notifying with law enforcement and government security agencies? | | | | |
| 26a. Do you routinely exercise your cyber response plans and procedures? | | | | If yes, how often? |
| 26b. Does this include working with law enforcement and government security agencies? | | | | |
| 27a. Do you perform post-event analysis? | | | | If yes, how is this recorded? |
| 27b. Does this include working with law enforcement and government security agencies? | | | | |
| 28. Do you incorporate lessons learned into your policies, plans, and procedures? | | | | |
| **RISK IDENTIFICATION AND MANAGEMENT**<br>29. Do you have an enterprise-wide all-hazards risk management strategy? | | | | |
| 30. Are your operations, cyber, and physical security teams engaged in your risk management strategy? | | | | |
| 31. Do you periodically conduct risk assessments, including outsourced vulnerability assessments, and are the results reported to you? | | | | If yes, how often and who are they reported to? |

| | | | | |
|---|---|---|---|---|
| 32a. Does your risk management strategy address cybersecurity supply chain risks? | | | | |
| 32b. Does your risk management strategy address insider threat risks? | | | | |
| **INFO SHARING & SITUATIONAL AWARENESS**<br>33a. Do you maintain and integrate situational awareness of operations, cyber and physical threats? | | | | |
| 33b. Do you maintain informational sharing relationships with external entities (both government and commercial) to collect and provide cybersecurity and physical security information? | | | | |

## Appendix A

FERC Group 1 Security Documentation Checklist (v2. 12/17/2014)

**Date of Inspection:** **Project Number/Name:** **Inspector :**

### FERC Security Requirements - Group 1

| Document | Required | Document Date | FERC Comments |
|---|---|---|---|
| **Security Plan** (update annually or if changes; exercised every 5 yrs) | X | | |
| **Vulnerability Assessment** (update annually; reassess every 5 yrs) | X | | |
| **Annual Security Compliance Letter** (due annually) | X | | |

### Documents to Review during Security Inspection (Group 1)

| Document | Required | Suggested | Verified | FERC Comments |
|---|---|---|---|---|
| **Site Security Plan (Physical/Operational)** | X | | | |
| **List of Restricted Areas** | | X | | |
| **List of Critical Dam Assets** | | X | | |
| **Physical Security Descriptions/Inventory** | | X | | |
| **Physical Security Layout/Drawings** | | X | | |
| **Security Operating Procedures** | X | | | |
| **Site Access Procedures** | | X | | |
| **Key Control Procedures** | X | | | |
| **Procedures for Civil Disturbance/Protests** | | X | | |
| **Bomb Threat Procedures/Response** | | X | | |
| **Procedures for Temporary Project Closure** | | X | | |
| **Threat Level Planning/Procedures (posture adjustments)** | X | | | |
| **Communication Procedures/Redundancies** | X | | | |
| **Information Technology (if applicable)** | X | | | |
| **SCADA (if applicable); NERC compliance, (if applicable)** | X | | | |
| **Security Equipment Testing, O&M** | | X | | |
| **Internal Emergency Response** (actions linking security to EAP) | X | | | |
| **Rapid Recovery Procedures** (discuss dam and all critical assets) | X | | | |
| **All Upgrades to Physical and Operational Security are included** | X | | | |
| **Site Vulnerability Assessment (VA)** | X | | | |
| **discusses Scope/Methodology/Assumptions** | | X | | |
| **discusses list of Critical Assets** | | X | | |
| **discusses Consequences of individual asset destruction** | X | | | |
| **discusses Vulnerability of individual assets** | X | | | |
| **discusses Likelihood of Attack of individual assets** | X | | | |
| **discusses Threat against individual assets** | X | | | |
| **discusses the five standard scenarios, at minimum** (see p.24) | X | | | |
| **discusses Security Protection for individual assets (site SA)** | X | | | |
| **discusses Site Security Risk and recommendations** | X | | | |
| **List of security recommendations (P&S) at site** (if applicable) | X | | | |
| **List of security upgrades at site, w/compl. date** (if applicable) | | X | | |
| **Annual Compliance Letter** | X | | | |
| **discusses compliance with SP, VA, SA reprints & annual updates** | X | | | |
| **discusses date of last exercise of SP** (every 5 years) | X | | | |
| **discusses confirmation of security contact information** | X | | | |

**NOTES:**

**Completion date of last FERC Staff DAMSVR (min every 5 years or the first year a new engineer is assigned to the project; see p.15 of guidance):____________________.**
**Completion date of FERC Project Security Memorandum (due annually for Group 1):__________________.**
**Reviewed By (Regional Manager):____________________________________. Date:_________________.**

# Appendix A

FERC Group 2 Security Documentation Checklist (v2. 12/17/2014)

**Date of Inspection:** **Project Number/Name:** **Inspector:**

| FERC Security Requirements - Group 2 (5-year inspection schedule) | | | |
|---|---|---|---|
| **Document** | **Required** | **Document Date** | **FERC Comments** |
| **Security Plan** (update annually, or if changes made) | X | | |
| **Security Assessment** (update annually; reassess every 10 yrs) | X | | |
| **Annual Security Compliance Letter** (due annually) | X | | |

| Documents to Review during Security Inspection (Group 2) | | | | |
|---|---|---|---|---|
| **Document** | **Required** | **Suggested** | **Verified** | **FERC Comments** |
| **Site Security Plan (Physical/Operational)** | X | | | |
| **List of Restricted Areas** | | X | | |
| **List of Critical Dam Assets** | | X | | |
| **Physical Security Descriptions/Inventory** | | X | | |
| **Physical Security Layout/Drawings** | | X | | |
| **Security Operating Procedures** | X | | | |
| **Site Access Procedures** | | X | | |
| **Key Control Procedures** | X | | | |
| **Procedures for Civil Disturbance/Protests** | | X | | |
| **Bomb Threat Procedures/Response** | | X | | |
| **Procedures for Temporary Project Closure** | | X | | |
| **Threat Level Planning/Procedures (posture adjustments)** | X | | | |
| **Communication Procedures/Redundancies** | X | | | |
| **Information Technology (if applicable)** | X | | | |
| **SCADA (if applicable); NERC compliance, (if applicable)** | X | | | |
| **Security Equipment Testing, O&M** | | X | | |
| **Internal Emergency Response** (actions linking security to EAP) | X | | | |
| **All Upgrades to Physical and Operational Security are included** | X | | | |
| **Site Security Assessment (SA)** | X | | | |
| **discusses Scope/Methodology/Assumptions** | | X | | |
| **discusses list of Critical Assets** | | X | | |
| **discusses inherent accessibility & visibility of each critical asset** | | X | | |
| **discusses Security Protection for individual assets** | X | | | |
| **discusses unarmed intruder, at minimum** (see p.26-27) | X | | | |
| **List of security recommendations (P&S) at site** (if applicable) | X | | | |
| **List of security upgrades at site, w/compl. date** (if applicable) | | X | | |
| **Annual Compliance Letter** | X | | | |
| **discusses compliance with SP, SA completion & annual updates** | X | | | |
| **discusses confirmation of security contact information** | X | | | |

**NOTES:**

**Completion date of last FERC Staff DAMSVR (min every 5 years or the first year a new engineer is assigned to the project; see p.15 of guidance):____________________.**
**Completion date of FERC Project Security Memorandum (due at a 5 year interval):______________________.**
**Reviewed By (Regional Manager):________________________________________. Date:____________________.**

## Appendix B (i)

## PROCEDURES FOR REPORTING SUSPICIOUS ACTIVITY

1. IDENTIFYING SUSPICIOUS ACTIVITY. Although it is often difficult to determine whether a local incident has a terrorist nexus, similar incidents of suspicious activity across many local jurisdictions may indicate the existence of a national threat (see below for examples).

2. REPORTING SUSPICIOUS ACTIVITY. It is suggested that you NOT report information related to a U.S. person's ethnicity, race, religion, or lawful exercise of rights guaranteed by the Constitution or Federal law unless reasonable grounds exist that show a direct relationship of such information to a specific criminal act or behavior that may pose a threat. It is also important to protect the rights of U.S. persons by ensuring personal information is not disseminated or disclosed to anyone who does not have the authority and need to access such information.

### CATEGORIES OF SUSPICIOUS ACTIVITY

1. ACQUISITION OF EXPERTISE: Unjustified attempts to obtain or conduct specialized training in security concepts, facility operation, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities.

2. BREACH OR ATTEMPTED INTRUSION: Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel. (e.g., police, security, or janitorial personnel).

3. ELICITING INFORMATION FOR AN UNLAWFUL PURPOSE: Suspicious questioning of personnel by any means about particular structures, functions, personnel, or procedures at the facility or infrastructure.

4. EXPRESSED OR IMPLIED THREAT: A threat to personnel or threatened damage to or compromise of a facility or infrastructure.

5. FLYOVER AND/OR LANDING: Suspicious overflight of and/or landing near a facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider)

6. MATERIALS ACQUISITION AND/OR STORAGE: Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; and/or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

7. MISREPRESENTATION: Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

8. RECRUITING: Building operations teams and contacts, personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to personnel, facilities, or forces in transit.

9. SABOTAGE, TAMPERING, AND/OR VANDALISM: Damaging, manipulating, or defacing part of a facility, infrastructure, or protected site.

10. SURVEILLANCE: Monitoring the activity of owner personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to personnel or facilities.

11. TESTING OF SECURITY: Interactions with or challenges to facilities, personnel, or systems that could reveal physical, personnel, or cyber security capabilities, including attempts to compromise or disrupt information technology infrastructure.

12. THEFT, LOSS, AND/OR DIVERSION: Theft or loss associated with a facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, copper wire, technology, or documents, whether classified or unclassified) that are proprietary to the facility, and/or a diversion of attention from a facility or infrastructure that is related to a theft or loss associated with that facility.

13. WEAPONS DISCOVERY: Discovery of weapons or explosives.

Federal Energy Regulatory Commission
Division of Dam Safety and Inspections
**FERC Security Program for Hydropower Projects**
***Revision 3 (Final 8/31/2015)***
**Appendix B (ii)**

## SAMPLE SUSPICIOUS ACTIVITY REPORTING FORM
## (Mark as: "Privileged – Security Sensitive Material")

Incident Entered By:____________________________
Originating Agency:____________________________
Originators Email Address:_____________________

---

Incident Title: (The incident title should be a short narrative similar to a news article headline that will summarize the activity)

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
_________________________________________

---

Agency Report #/ID:____________________________
Reporting Officer:______________________________
Date of Incident:_______________________________
Time Incident Observed:_________________________
Time Zone Incident Observed:____________________

---

Incident Type: (For incident type, chose one of the Categories that are listed in the Suspicious Activity guidance)____________________

Incident Sub-type: (For example, if the incident type is Surveillance, then the Sub-type could be photography or video) _____________________________

---

Incident Summary: (The incident summary is the body of your report. Provide as much detail as possible here about the incident).

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
_________________________________________________________________________________

Action Taken: (List any coordination with law enforcement, law enforcement or other actions taken)

______________________________________________________________________________

___________________________________________________________

Incident Location:
Name of Location:

______________________________________________________________________________

______________________________________________________________________________

_________________________________________________

Type of Location:

______________________________________________________________________________

___________________________________________________________

Address of Location:

______________________________________________________________________________

Submit any applicable attachments with this report. Depending on the nature of the SAR, terrorism-related and other cyber or criminal threat information included within may be submitted to eGuardian for investigation by the FBI. eGuardian is a database developed and operated by the FBI and is limited to users who have a need-to-know and who undergo a strict vetting process. SAR information will not be further distributed without the express consent of the originating agency. A complete report greatly assists the investigation process. In particular, information such as incident location, type of incident, and any other identifying information can greatly increase the FBI and/or other law enforcement entities chances of conducting a complete investigation. It is possible that the FBI may require additional information; for this reason, the POC identified on the SAR may be contacted.

## Appendix C

## EXAMPLES OF THREAT RESPONSE ACTIONS FOR LICENSEES

**Normal Condition**

There is no credible, specific, or impending terrorist threat against the United States. The following protective measures can be considered:

**1. EMPLOYEES**

- Perform background checks (level of detail determined by the licensee) 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.
- Review all operations plans and orders, EAPs, Recovery Plans, and Standard Operating Procedures (SOPs).
- 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**

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

## Elevated Threat Alert

“Elevated” warns of a credible terrorist threat against the United States. It is “Elevated” if the United States has no specific information about the timing or location. 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. Stress importance of vigilance.
- 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. Notify local police if access/road closings could impact their operations in the local community.

**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. At beginning and end of each workday and at frequent intervals, inspect interior and exterior of buildings in regular use for suspicious packages, or signs of tampering, or indications of unauthorized entry.
- Cancel non-essential deliveries.
- Cancel non-essential maintenance/construction that utilizes non-company workers.

**Imminent Threat Alert**

"Imminent" warns of a credible, specific, and impending terrorist threat against the United States. It is "Imminent", if the United States believes the threat is impending or very soon. 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. Erect barriers, as necessary.
- 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. Conduct unannounced security spot checks.

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

## DAMSVR

The Federal Energy Regulatory Commission (FERC) is the distribution center for the DAMSVR document, and all requests for copies of DAMSVR may be made to FERC as described below.

Any organization or person demonstrating a legitimate need to obtain a copy of DAMSVR will be provided a copy via electronic means. The FERC reserves the right to refuse distribution of DAMSVR to any organization and/or person if they cannot demonstrate a need to have the document (ref. Order No. 630, 630-A, Critical Energy Infrastructure Information at: http://www.ferc.gov/legal/ceii-foia/ceii.asp)[4]. An organization or person may request a copy by visiting the FERC website at:
http://www.ferc.gov/industries/hydropower/safety/guidelines/security.asp

Follow the links for a "Request for DAMSVR" and complete the online forms. Only one person from an organization should request DAMSVR from FERC. Each organization or person requesting a copy of DAMSVR must designate this person as the single Point of Contact (POC), who will be responsible for requesting copies from FERC and for distribution of DAMSVR within his/her organization, and only to those employees with a need to have a copy. While requesting DAMSVR online, you will need to provide your name, organization, position, stated need for the document, and your intended use of the methodology. When the request is completed, your organization will be registered as a DAMSVR user. In most cases, a copy of DAMSVR will be sent within five working days of a request. The POC can distribute DAMSVR only to employees within his/her organization, and if asked to provide copies from personnel outside their organization, they should direct the requestor to the FERC website as noted above.

It is anticipated that DAMSVR will be continually reviewed in order to provide the best product possible. FERC will retain the most current version of DAMSVR. Each copy of DAMSVR contains a Revision/Date Number and FERC will make every attempt to provide currently registered users with the latest version. The current Revision/Date Number will be posted on the FERC website at:
http://www.ferc.gov/industries/hydropower/safety/guidelines/security.asp

Users of DAMSVR are encouraged to refer to this site periodically to ensure that their copy is current. If your organization does not have the most current version of DAMSVR, your POC can request a revised copy via the same link described above. POCs are also encouraged to provide methodology feedback to FERC via the above link.

**[4] DAMSVR, although intended as a security assessment methodology, contains information and procedures that could potentially be used to plan an attack against a dam. As such, DAMSVR should be treated as a sensitive document and should only be provided to users demonstrating a need to have the document. Distribution of this document outside your organization is not authorized.**

## Appendix E

## INTERNAL EMERGENCY RESPONSE AND RAPID RECOVERY PLAN FORMAT[5]

Below is a suggested Table of Contents for an Internal Emergency Response and Recovery Plan Format (Draft). *This Internal Emergency Response and Rapid Recovery Plan (IERRRP) is designed as a separate document which can supplement the primary Emergency Action Plan (EAP) and be part of a project's Security Plan. Whereas the primary EAP is designed to facilitate early warning and evacuation of potentially affected downstream areas, this document deals with MITIGATION AND EMERGENCY REPAIR OF AFFECTED COMPANY STRUCTURES AND PLANT FACILITIES. This plan should be utilized for any emergency arising at the site, whether from natural or manmade causes. The content of the Recovery Plan should avoid duplication of existing plans (such as the EAP) as much as possible. The Recovery Plan is intended for internal use and response only.*

**Sample Table of Contents:**

I. Purpose of Internal Emergency Response and Rapid Recovery Plan **(Security Group 1 Dams)**

**Internal Emergency Response Plan:**

II. Incident Command System (ICS) & Company Internal Assignments/Responsibilities
   a. Incident Command System (ICS)
   b. ICS Chart: Company Personnel Assignments
   c. Incident Command Post and Alternate Command Post
   d. Personnel at On-Site Incident Command Post
   e. Main Headquarters Emergency Personnel
   f. Media Contact (Public Information Officer)

III. Coordination with Local Authorities
   a. Multiple-Jurisdiction Incident (Unified Command)
   b. Safety/Clearance Issues & Authorization

IV. Communications, Maps, and Drawings
   a. Communications Center
   b. Alternate Communications Methods (cell phone, radios)
   c. Drawings, Maps, Photographs

[5] **Appendix E is referenced from the DHS Dams Sector Crisis Management Handbook, A Guide for Owners and Operators 2015.**

V. Response Times & Geographical Limitations
   a. Call-out Procedure
   b. Estimated Response Times
   c. Primary & Secondary Access Roads & Alternatives
   d. Staging Areas for Personnel & Equipment

VI. Meals & Lodging
   a. Company Living Facilities
   b. Local Restaurants & Motels

VII. Internal Maintenance of Plan

**Rapid Recovery:**

VIII. Applicable Emergency Scenarios (listed for each scenario is primary concerns, materials/equipment needed, & operating procedures)
   a. Overtopping (including excessive inflow or reservoir displacement)
   b. Earthquake Damage
   c. Loss of Dam Crest Length
   d. Slide on Upstream or Downstream Slope of Embankment
   e. Slide on Underlying Potential Failure Plane
   f. Excessive Settlement
   g. Sinkhole Activity
   h. Loss of Foundation or Abutment Material (such as landslide/rockfall)
   i. Excessive Seepage/Piping through Embankment, Foundation, or Abutments
   j. Failure of Appurtenant Structure Such as a Spillway Gate
   k. Excessive Cracking in Concrete Section
   l. Penstock Rupture/Failure
   m. Turbine or Other Equipment Failure
   n. Vandalism/Bomb Threat/Terrorism
   o. Other

IX. Vehicles, Equipment, Materials (e.g., sandbags, concrete, rip rap) & Contractors
   a. Plant On-Site Inventory
   b. Other Available Company Vehicles, Equipment, Materials, & Supplies
   c. Non-Company Supplies/Materials (including helicopters if necessary)

Outside Contractors and Consultants

Federal Energy Regulatory Commission
Division of Dam Safety and Inspections

## FERC Security Program for Hydropower Projects

***Revision 3 (Final 8/31/2015)***

## Appendix E

I. Purpose of Internal Emergency Response Plan **(Security Group 2 Dams)**

**Internal Emergency Response:**

II. Incident Command System (ICS) & Company Internal Assignments/Responsibilities
  a. Incident Command System (ICS)
  b. ICS Chart: Company Personnel Assignments
  c. Incident Command Post and Alternate Command Post
  d. Personnel at On-Site Incident Command Post
  e. Main Headquarters Emergency Personnel
  f. Media Contact (Public Information Officer)

III. Coordination with Local Authorities
  a. Multiple-Jurisdiction Incident (Unified Command)
  b. Safety/Clearance Issues & Authorization

IV. Communications, Maps, and Drawings
  a. Communications Center
  b. Alternate Communications Methods (cell phone, radios)
  c. Drawings, Maps, Photographs

V. Response Times & Geographical Limitations
  a. Call-out Procedure
  b. Estimated Response Times
  c. Primary & Secondary Access Roads & Alternatives
  d. Staging Areas for Personnel & Equipment

VI. Meals & Lodging
  a. Company Living Facilities
  b. Local Restaurants & Motels

VII. Internal Maintenance of Plan

Appendix A: List of Company Response Personnel (internal call-out list of phone numbers)
Appendix B: List of Contractors/Consultants (addresses and phone numbers)
Appendix C: List of Equipment Suppliers (addresses and phone numbers)
Appendix D: Local Restaurants & Motels (addresses and phone numbers)
Appendix E: Other Utilities/Mutual Aid (phone numbers of key contacts)
Appendix F: Federal/Governmental Assistance (phone numbers of key contacts)
Appendix G: Engineering Key Drawing List (drawings are located in two secure, non- inundated areas near the facility)
Appendix H: Highway Maps and Photos of Dam
Appendix I: Emergency Helicopter Rescue Numbers
Appendix J: Bomb Threat Procedures
Appendix K: EAP Flowcharts A and B (identical to those in the regular EAP) Guidance for the Preparation of the Recovery Plan

Sections I through IX (not including appendices) could total less than 25 double-spaced pages. This document (like the Security Plan) is not required to be actually submitted to the FERC. FERC Engineers could ask to examine the plan during the annual inspections and comment on its acceptability. The FERC suggests that this document, when prepared, be marked as “Privileged - Security Sensitive Material.”

The Recovery Plan is primarily developed for the benefit of the dam owner, but also will be beneficial to the region or country in rapidly reinstating essential project benefits. Having a comprehensive plan enables licensees to more quickly mitigate, recover, and "get back on line" following a serious structural incident at a facility. It makes good business sense for a licensee to formulate a Recovery Plan for those facilities that would (if they failed) most seriously impact the licensee's generating capability and/or bottom line economic benefits. Recovery Plans are not necessarily applicable for every High Hazard Potential facility.

The recovery phase should begin as soon as possible after the catastrophic event (dam failure, loss or damage to powerhouse, loss of main transmission line, etc.) and usually overlaps the “response phase” of the event. Planning and actions during the “response phase” should consider any actions which might be implemented to return the development to service. Recovery phases include “initial” (within one week) and “long-term” activities (recovery could continue for months), depending upon the magnitude of impact on hydroelectric facility operations, including dams, powerhouses, and water conveyance.

## Section I. Purpose of Internal Plan

This Internal Emergency Recovery Plan (IERP) is designed as a separate document which can supplement the primary Emergency Action Plan (EAP). Whereas the primary EAP is designed to facilitate early warning and evacuation of potentially affected downstream areas, this document deals with mitigation and emergency repair of affected company structures and plant facilities. A Recovery Plan should be prepared on a site-specific basis in that different facilities (i.e., dams and associated structures) will require different considerations. This is not intended to be a company-wide Continuity of Operations Plan, but rather a plan to bring a specific facility back in operation as efficiently as possible. It is intended for internal use and response only.

**Rapid Recovery (Security Group 1 Dams)**

<u>Section II. Applicable Emergency Scenarios</u>

Each "Applicable Emergency Scenario" need only be one page in length, including materials/equipment needed and operating procedures. A universe of potential emergency scenarios need not be listed for each facility, but rather should be tailored to the site-specifics of the facility. For example, “Overtopping” may be a minor concern for a facility designed to accommodate flows over the entire structure. A good start in developing applicable emergency scenarios is the Potential Failure Modes Analysis (PFMA) document prepared for the facility, although all applicable scenarios, such as terrorism, may not be covered in the PFMA.

Each critical component for the applicable scenario should be identified with the likely range of potential hazards and consequences. Predict the type and magnitude of damage, and develop a list of options to minimize the consequences, either by reducing initial damage, or by limiting progression of the initial damage, or by reducing the time needed to repair the damage. Results of this effort should be consolidated into a list of recommended actions that might include procurement, stockpiling, on-the-shelf designs, or general preparedness actions. An example of what a component analysis could entail is shown in Attachment 1.

Another important consideration to address is the role and responsibility of the dam owner personnel to respond to the emergency, both in an initial and a long-term basis. Things to consider include (but are not necessarily limited to):

**<u>Initial Recovery</u>**

- If the Emergency Action Plan is still activated, determine appropriate time to terminate EAP and transition to Recovery phase. Define requirements for interim inspection and monitoring above and beyond the Standard Operating Procedures.
- Restore critical systems (generation facilities, dams, water conveyance systems, telecommunications, monitoring systems, controls, etc.) to stable and safe operations. Assure public safety and business continuity.

- Evaluate the need to continue the Emergency Management Organization (the Leadership team put in place by activation of the Emergency Action Plan), and transition back to normal organizational structure, roles and responsibilities as soon as feasible.
- Complete detailed condition assessment of all relevant facilities, equipment and operations.
- Coordination with other agencies for the mitigation of the emergency, especially for environmental concerns.
- Conduct after-event critiques and debriefings as soon as practical; provide incident reports to Company Management and Regulatory Agencies.
- Consider appointing a Recovery Team (members experienced with evaluation of structures, systems, equipment and operations; this team would develop the alternatives to be evaluated and approved for returning to normal operations) to plan and oversee the long-term recovery process.
- Establish priorities for permanent repair, reconstruction, or replacement at existing or new locations.
- Complete an assessment of losses and an analysis of costs for repairs versus replacements.
- Review and define needs for additional specialized technical resources and temporary staff, including additional security staff if necessary, and initiate procurement/recruitment process.
- Arrange for orientation and training of any temporary staff.
- Determine approximate reimbursements from insurance and other sources of financial assistance, and identify alternatives for financing residual costs.

## **Long-Term Recovery**

- Revise Operational Plans, Emergency Action Plans, Disaster Recovery Plans, and Manuals as appropriate.
- Identify any enhancements that should be made to hydroelectric facility components and/or operations, and establish strategy for long-term recovery and environmental restoration.
- Establish and maintain liaison with federal, state, and local government agencies for inspections, permits and reconstruction as necessary.
- Initiate permanent reconstruction of damaged facilities and replacement of damaged equipment.

## Internal Emergency Response (Security Group 1 and 2 Dams)

### Section III. Incident Command System (ICS) & Company Internal Assignments/Responsibilities

The purpose of this section is to describe the emergency response structure the dam owner will operate within and briefly discuss the roles and responsibilities expected from personnel internal to the dam owner's organization.

### Section IV. Coordination with Local Authorities

This section should briefly discuss what the dam owner needs to do to coordinate with local law enforcement and emergency response personnel they will work with, and any special needs they have identified. The complet3e list of applicable agencies would be included in Appendix, the EAP Flowcharts.

### Section V. Communications, Maps, and Drawings

This section should list how communications will occur throughout the emergency, list alternate communication sources, and include a brief section with pertinent maps, drawings and photographs that would be useful to have during an emergency. Maps, drawings and photographs may be included in Appendices G and H.

### Section VI. Vehicles, Equipment, Materials (e.g., sandbags, concrete, rip rap) & Contractors

This section should list all the vehicles, materials and equipment the dam owner would need to respond to the applicable emergency scenarios identified in Section II. A current list of contractors and support personnel that can be utilized during the emergency should also be listed in this section for easy reference.

### Section VII. Response Times & Geographical Limitations

Anticipated response times, call-out procedures and geographic limitations should be addressed in this section. Clearly defined directions to critical areas and other locations should be included in textural and graphical format. Staging areas and security exclusion zones should also be identified.

### Section VIII. Meals & Lodging

Any logistical considerations for sustaining personnel detailed to temporary quarters should be identified in this section.

### Section IX. Internal Maintenance of Plan

This section should address how the Recovery Plan is maintained (updated). Internal employee training of the procedures and information contained within the Plan should also be defined.

Federal Energy Regulatory Commission
Division of Dam Safety and Inspections

# FERC Security Program for Hydropower Projects

***Revision 3 (Final 8/31/2015)***

## Appendix E

Appendices

The most critical section of the Plan is the Appendix section (the "nuts and bolts" that helps mitigate/recover from the emergency). The appendices could probably suffice by themselves as the "recovery" plan for most licensees. They contain information that most dam owners undoubtedly (and hopefully) already have on file somewhere to mitigate an emergency. This information is simply consolidated into a single document. Appendices should be designed so that critical information contained therein may easily be verified and updated on an annual basis.

### Attachment 1

### Examples of Component Analysis

**Component:** Switchyard transformer
**Likely type/magnitude of damage:** Ballistic damage to shell and windings
**Consequences of damage:** No immediate loss of hydropower transmission, due to availability of redundant transformer capacity. Less reliable system until transformer is replaced (normal 18 month replacement time); possible power loss would represent a very small percentage of regional capacity
**Options to minimize consequences:**
1. Rely on existing redundant transformer capacity
2. Install additional redundant capacity
3. Emergency procurement of new transformer (9 months)

**Recommended option:** #1, but this will limit system reliability until a new transformer is online
**Component:** Tainter gates
**Likely type/magnitude of damage:** Trunion pin failure deforms gate, making gate inoperable **Consequences of damage:** Until gate is replaced (normal 14 month replacement time) loss of pool, reduction of recreation, loss of power production
**Options to minimize consequences:**
1. Procure and store a spare gate (2 week recovery)
2. Emergency procurement of a new gate (9 months)
3. Procure and store a bulkhead to restore pool until new gate is installed

**Recommended option:** #3, bulkhead will be suitable for use at 5 company projects