**Company Name**

**Company Address**

***\*\*\*anything* bolded *must be addressed by the licensee, anything bolded and italicized is for guidance and should be removed from your finalized submittal\*\*\****

 **December DD, 20YY**

**Mr./Ms.** **(Regional Engineer)**

**FERC D2SI Regional Office**

**Address**

Re: 20**YY** (Current year) FERC D2SI Security Compliance Certification for: **Development(s) *(name/numbers; e.g. Development Name 1, P-00999-01; Development Name 2, P-00999-02; etc.; The Development(s) listed here should match Attachment 1(details in footnotes). If you have 5 Developments or less, then list them; if you have six or more Developments list the first Development numerically and use et al***.**; *Do not put the Security Group classification in the Subject line).***

**Mr./Ms.** **(Regional Engineer)**:

***Please read the information below carefully. Do not adjust or edit anything below (until the signature section). The language is standardized for any/multiple Security Group 1, Security Group 2, and interconnected (cyber) Security Group 3 Development(s) to certify compliance. If your program does not conform to the information below, then your program is not in compliance with the FERC security program. If that is the case, then submit the specific deficiencies and a plan and schedule to address them in lieu of the Annual Security Compliance Certification.***

We are certifying compliance to the [FERC Security Program for Hydropower Projects Revision 3A](https://www.ferc.gov/sites/default/files/2020-04/security.pdf) for the referenced Development(s) above and further detailed in Attachment 1- Security Documentation Table.

Each of our Security Group (SG) 1 and/or 2 Development(s) have their own site specific: Security Plan with an Internal Emergency Response (SG1 and SG2 requirement) and Rapid Recovery Plan (SG1 requirement only), Vulnerability Assessment (SG1 requirement only), Security Assessment (SG1 and SG2 requirement). In addition, we further detail that:

* The Security Plan(s) (SP) for above referenced Development(s) have been reviewed for the current year and are compliant with the annual update requirement as verified in Attachment 1- Security Documentation Table.
* The Internal Emergency Response Plan(s) (SG1 and SG2 requirement) and/or Rapid Recovery plan(s) (SG1 requirement only) for above referenced Development(s) have been reviewed for the current year and are compliant with the annual update requirement as verified in Attachment 1- Security Documentation Table.
* The applicable Security Plan(s) for above referenced Development(s) have fulfilled the exercise requirements and schedule (SG1 requirement only; every 5 years; at a minimum of a drill level) as verified in Attachment 1- Security Documentation Table.
* The Vulnerability Assessment(s) (VA) (SG1 requirement only) for above referenced Development(s) have been reviewed and updated for the current year; and are compliant with the 5-year re-evaluation/re-print (or when site conditions change) as verified in Attachment 1- Security Documentation Table.
* The Security Assessment(s) (SA) (SG1 as part of the VA and SG2 Development(s) for above referenced Development(s) have been reviewed and updated for the current year; and are compliant with the 10-year re-evaluation/re-print (or when site conditions change) as verified in Attachment 1- Security Documentation Table.
* Cyber Security for the applicable above referenced Development(s) and those interconnected were reviewed and the cyber security checklist(s) are current. ***(SG3 Developments that are interconnected with other critical or operational cyber Developments must have a site-specific checklist)***
* Cyber Security for the applicable above referenced Development(s) and those interconnected were reviewed/evaluated as detailed in Attachment 2-Cyber Asset Designation Sheet. ***(SG3 Developments that are interconnected with other critical or operational cyber Developments must be listed on Attachment 1 and detailed in Attachment 2)***
* Implementation status of Baseline and/or Enhanced Cybersecurity Measures are detailed in Attachment 2-Cyber Asset Designation Worksheet.
* We have provided the FERC Security Checklist(s) (version 5/5a; SG1 and SG2 requirement) for all applicable Development(s) in Attachment 3 ***(you must provide a site-specific checklist for all SG1 and SG2 Developments; e.g. one for each Development. You may optionally provide site-specific checklists for SG3 Developments.***

Security Correspondence for our Development(s) can be found in Attachment 4-Security Correspondence ***(see directions in Attachement-4 below)***. If you have any questions related to this certification, please feel free to contact me.

Sincerely,

**Signature**

**Name**

**Title**

**Address**

**Phone (Office/Cell)**

**Email**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project/Development****Name**1 | **Project-Development No.**1 | **FERC Security Group**1 |  **Security Plan****Annual****Review- Update**2 | **Internal Emergency Response Plan Annual****Review- Update**2 | **Rapid Recovery****Plan Annual****Review- Update**2,3 | **Security Plan** **5-Year****Exercise**2,3 | **Vulnerability Assessment Annual Review- Update**2,3 | **Vulnerability Assessment** **5-Year** **Re-eval-****Re-print**2,3 | **Security Assessment Annual Review- Update**2 | **Standalone** **Security Assessment** **10-Year****Re-eval-****Re-print**2,4 |
| Any Dev Name 1  | #####-## | # | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY  |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY  |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY  | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY  |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY | MM/DD/YYYY  |
|  |  |  |  |  |  |  |  |  |  |  |

***\*\*\* Add or Delete as many rows as necessary\*\*\****

1 For the majority of licensees usually only SG1 and SG2 developments are required to be listed; however, SG3 developments that are remotely interconnected with other SG1 or SG2 developments that have a cyber designation of critical or operational must be listed in this field with **no asterisk**. You are not required to list any SG3 developments that are not interconnected with a critical or operational cyber asset; however, if you want to optionally list your non-interconnected SG3 developments then you may do so by using **an asterisk**.

2 Indicates optional documentation fields for SG3 developments regardless of cyber interconnectivity. If you have voluntarily completed the optional documentation, then input the date with an asterisk (MM/DD/YYYY\*); otherwise input “NA”.

3 Indicates optional documentation fields for SG2 developments. If you have voluntarily completed the optional documentation, then input the date with an asterisk (MM/DD/YYYY\*); otherwise input “NA”.

4 The Standalone Security Assessment 10-year Reevaluation/reprint is required for SG2 developments. SG1 security assessments are updated every 5-years as part of the VA. If you are a SG1 development, you can either enter the same date that is in your VA 5-year Re-eval-Re-print column or input “NA”.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project/Development Name** | **Project -Development No.** |  **FERC Security Group**  | **Inspection Date 1** | **Physical Feature 2 (e.g. spillway gate(s), powerhouse, low-level outlets, etc.)** | **Cyber Asset Designation (Critical, Operational, Non-Critical)** | **NERC Regulated (High, Medium, Low, or no) 3** | **Most Recent NERC Audit Date** | **Status to implement baseline and/or enhanced measures 4** | **Notes 5,6** |
| Any Dev Name 1  | #####-## | # | MM/DD/YYYY |  |  |  | MM/DD/YYYY | Complete; MM/DD/YYYY |   |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY |  |  |  | MM/DD/YYYY | Incomplete, MM/DD/YYYY\* |   |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY |  |  |  | MM/DD/YYYY | Complete; MM/DD/YYYY |   |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY |  |  |  | MM/DD/YYYY | Complete; MM/DD/YYYY |   |
| Any Dev Name 1 | #####-## | # | MM/DD/YYYY |  |  |  | MM/DD/YYYY | Incomplete; MM/DD/YYYY\* |   |
|  |  |  |  |  |  |  |  |  |  |
|  |

***\*\*\* Add or Delete as many rows as Necessary\*\*\****

1 Most recent FERC-D2SI Security Inspection conducted by the Security Branch Specialist. Security Review by FERC Dam Safety engineer does not count.

2 Physical features operated over networks.

3 Indicate if the physical feature is operated by a BES Cyber System as categorized under NERC CIP-002-5.1a, and if so, what the designated impact rating is. If there are systems of multiple impact ratings that apply, list the highest impact rating.

4 Indicate complete and input the date (MM/DD/YYYY) that baseline and/or enhanced measures were implemented.

5 Justify the reasoning for cyber asset designation as critical, operational or non-critical; For example, explain consequences from a cyber attack in relation to losing generation, releasing the reservoir, loss of water supply, etc.; Discuss project's interconnection. If cyber asset is non-critical, indicate the following: locally operated, remotely operated or with automated operations and confirm there are no consequences. If cyber asset is non-critical, it needs to be reassessed annually to account for changes in operating conditions.

6 For assets subject to the NERC Reliability Standards, discuss if there are BES Cyber Systems of different impact ratings (per CIP-002) that facilitate the operation of the listed physical feature, or if control systems in the hydro project are isolated from those subject to NERC CIP. Also include the status of mitigation plans for CIP audit non-compliances and areas of concern from the most recent audit.

**FERC SECURITY CHECKLIST (v5a)**

**Field Security Inspection Form 1**

**Project-Development No.: Proj/Dev Name: Licensee:**

**Security Group: Date: Inspector/Attendees:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Field Observations: (Provide detailed supplemental information to the right)** | **Y** | **N** | **NA** | **Comments****(Provide additional details – especially any “No” answers – here and separate sheets, if necessary.** **Indicate NA if not appropriate to site.)** |
| **DETECTION AND ASSESSMENT**1. Is the site manned? Dam? |  |  | Days/week Hours/day . ***note hours of operation and days*** |
|  Powerhouse? |  |  | Days/week Hours/day . ***note hours of operation and days*** |
| 2. Are there surveillance Dam? cameras in use?  |  |  |  | ***Note number of cameras, type of cameras (and if detection isintegrated), and location.*** |
|  Powerhouse? |  |  |  | ***Note number of cameras, type of cameras (and if detection isintegrated), and location.*** |
|  Other? |  |  |  | ***Note number of cameras, type of cameras (and if detection isintegrated), and location.*** |
|  How are they viewed/checked? | Operator – ***Describe where and how cameras are monitored.***  |
| 3. Is the frequency of walking inspections appropriate (safety and/or security)? |  |  |  | Note the frequency of these inspections:  ***Describe what is being inspected, by whom.*** |
|  Personnel control/ID badges used? |  |  |  | ***Discuss policy for ID badges.*** |
| **DELAY**4. Is the dam site fenced with gates/doors locked (if appropriate to the site)? |  |  |  | ***Describe type of fence, how things are locked, devices to lock. When areas are open/unlocked (e.g. unlocked during working hours, locked at all times, etc.).*** |
| 5. Is access restriction to the Foot? dam/facilities appropriate  and in-place?  |  |  |  | ***Describe condition of fencing and whether or not an adversary can breach the perimeter by foot. Discuss open areas where no perimeter fence is available.***  |
|  Vehicle? |  |  |  | ***Describe condition of fencing and whether or not an adversary can breach the perimeter by vehicle. Discuss open areas where no perimeter fence/gate is available.***  |
|  Boat? |  |  |  | ***Describe boat barriers if available. Note: buoy systems cannot stop a boat.*** |
| 6. Are spillway/gate controls secured against unauthorized access? |  |  |  | ***Describe how it is locked and material used to lock – e.g. steel cover with lock.*** |
| 7. Are powerhouse doors/ windows locked? |  |  |  | ***Describe locking mechanisms, technology, access control, etc.…*** |
|  Alarms/motion detection/cameras? |  |  |  | Specify details:  ***Discuss technology used, where it is located and what it is protecting.*** |
|  Can systems be easily bypassed? |  |  |  | ***Be careful when answering yes, remember system must be integrated and have the capability to deter, detect, assess, delay and respond to a threat – 360-degree security.*** |
| 8. Water conveyance Access restricted? system: |  |  |  | ***Describe how access is restricted to critical features such as intake structures and outlet works for foot and vehicle traffic.*** |
|  Surveillance? |  |  |  | ***Describe number of cameras, type of cameras, location of cameras, and it field of view.*** |
| 9. Is critical performance monitoring equipment secured against tampering? |  |  |  | ***Describe how instrumentation is protected.*** |
| **Field Observations** | **Y** | **N** | **NA** | **Comments** |
| **RESPONSE**10. Are law enforcement phone numbers posted? |  |  |  | ***Describe where numbers are posted, is it easily accessible?*** |
| 11. Are there redundant communications? |  |  |  | ***Describe redundant means of communication if primary fails.*** |
| 12. How long it takes the operator if detected to respond to unauthorized access? | How is detection made?  ***Describe technology for detection and the procedure following detection.*** |
|  What is that response? | ***Describe the response whether it is an operator responding, guards, or law enforcement.*** |
| 13. Can law enforcement be quickly notified? |  |  |  | Identify enforcement agenc(ies): & capabilities:  ***Describe all responding LE agencies and their fire power (e.g. SWAT team).*** |
|  Estimated time for arrival? |  |
| **INTEGRATION & RISK MANGMT.**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. | ***Describe threat assessment if one has been completed and with which agency/security consultant conducted it. Discuss weakest points of development and possible impacts. Don’t be too specific as this would be reflected in the VA.*** Last time consultation with law enforcement was made to determine threat:  ***Provide date and Law Enforcement Agency/Agencies*** |
| 15. Steps taken to improve Past year: security: | ***Describe physical security and procedural improvements.*** |
|  Long term plans: | ***Describe long-term plans – also captured in VA/SA recommendations.*** |
| 16a. Is there a Security Plan? (Group 1 or 2) |  |  |  | If “Yes” is it acceptable?  ***Ensure SP is a useable set of procedures.***Is there a Response/Recovery Plan component?  ***EAP can also help in developing this section in SP.*** |
|  Are there different site-specific response levels covered in the Security Plan for varying threat? |  |  |  | Summarize levels/activities:  ***We are following the DHS NTAS -Normal, Elevated, and Imminent threat levels. Briefly describe security enhancements during changing threat levels.*** |
|  Are the measures on the day of  inspection consistent with the  current threat level? |  |  |  | If “no” explain:  ***Describe what current threat level is and the actions taken to mitigate against threat.*** |
| 16b. Has Security plan been revised since last field change? |  |  |  | ***Briefly describe changes to procedures.***When it was last exercised & what type?  ***Date of last exercise (SG1), and type (e.g. drill, tabletop, functional, full scale). State is SP was exercised in conjunction with EAP exercise***.  |
| 17. Is there a Vulnerability Assessment? (Group 1) |  |  |  | If “Yes” is it compliant?  ***Ensure VA addresses all of the requirements of the FERC Security Program, specifically assessing consequence, vulnerability, likelihood of attack against all 5DBTs for each critical asset.*** |
| 18. Is there a Security Assessment?  (Group 1 or 2) |  |  |  | If “Yes” is it compliant?  ***Ensure SA addresses all of the requirements of FERC Security Program – accurately assess security effectiveness, develop list of recommendations for improvement.*** |
| 19. Are all actions and plans fully integrated? |  |  |  | ***Be careful when answering “yes.” Must have 360-degree security for the capability to deter, detect, assess, delay, and respond effectively.*** |
| 20. Do any security measures conflict with any license requirements |  |  | ***If yes, describe what the conflicts are. E.g. closing off recreation area to public based on security concerns. Must be coordinated with Regional Office/Security Branch.*** |
| 21. Is there HAZMAT/fuel storage on-site? |  |  | Describe:  ***What type of HAZMAT/fuel is on-site.*** |
|  If so, is access secured? |  |  | ***Describe how it is stored and secured.*** |
| 22. Are critical drawings/plans/records secured from unauthorized access? |  |  |  | ***Describe InfoSec procedures. How do employees access critical drawings?*** |
| 23. We have no comments about the Security Measures observed: |  |  | If no comments, check “No”; if comments needed, check “Yes”.  ***Describe any deficiencies in security system/program.*** |
|  If comments needed, follow-up actions will be made and tracked | List potential remediation discussed:  ***Describe recommendations for improvement.*** |

**Project Security Summary Information – Form 2**

|  |  |
| --- | --- |
| **Security Information** | **Comments****(Provide detailed information on separate sheet, if necessary)** |
| A. Number of security/surveillance incidents in past year.  ***Provide a number*** | Description (indicate if it was it reported to FERC) ***Discuss event that have occurred, what the results were, and whom the event was reported to (e.g. LE agency and which FERC Regional Office).*** |
| B. Owner expressed specific security concerns or questions. | ***Describe any security concerns that you may have for your development.*** |
| C. Number (description) of data requests or site visits by DHS PSA or other assessment groups.  ***Provide number*** | ***Briefly describe level of assessment conducted by DHS PSA or other assessment group and date of assessment.*** |
| D. Changes made to security since last inspection: | Indicate “None” by checking here: .Do previous studies show prior posture was adequate?(y/n) ***Describe effectiveness of security enhancement/procedural changes.*** |
|  Following changes were made to physical site security: | If so, describe changes:  ***Describe changes to physical security, any enhancements for physical security – should be captured in SP and VA/SA.*** |
|  Following changes made to procedural operations (incl. threat level increase additions, employee actions, etc.): | If so, describe changes:  ***Describe changes to security operating procedures for changing threat levels and the effectiveness of changes.*** |
|  Following changes/additions made to cyber/SCADA operations: | If so, describe changes:  ***Briefly describe operations whether or not site is operated manually or remotely through SCADA system. Identify criticality of cyber assets (non-critical, operational, critical). Briefly discuss cybersecurity measures and/or enhancements for SCADA protection.*** |
|  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).  ***Look at DAMSVR results and provide current and improved ASR values here based on security enhancements (mitigation). Describe how ASR was lowered.*** |
| E. A discussion was made with site personnel regarding no security materials submittal to eLibrary, and electronic mail (PW protected) only submittal of annual security compliance certification letter. | Yes, discussion was made (check if so): .***Self-explanatory***No, discussion was not made (reason why).  |

***\*\*\*There should be one Checklist per Development. Copy The 3 pages above and Paste as many checklists as needed here. You might have to readjust the top of the page to get it down to the next page\*\*\****

Security related correspondence for the referenced Developments listed in Attachment 1-Security Documentation Table can be coordinated through: ***(the Primary Security Contact and Secondary Security Contact are required per Development; i.e. 2 contacts at a minimum and 5 contacts at a maximum per Development; It is important to note that the formal contact list will be automatically updated once a year via the annual certification. If you would like to add or remove a person from formal contact list in between this cycle, then you must formally submit an Annual Security Compliance Certification Amendment with the Commission.)***

**Security Contacts for Specific Development Numbers XXXXX-XX, XXXXX-XX, and XXXXX-XX:** (***If you have different security contacts across your portfolio of Developments then you must delineate using this sub-header and duplicate as many times as needed. If all your Developments have the same security contacts, then delete this sub-header and the contacts you list below will be applied to all the developments listed in Attachment 1- Security Documentation Table)***:

|  |  |
| --- | --- |
| Primary Security Contact Name TitleCompanyAddress###-###-#### (Office)###-###-#### (Cell)Email | Secondary Security Contact Name TitleCompanyAddress###-###-#### (Office)###-###-#### (Cell)Email |
| Alternate Contact 1 Name TitleCompanyAddress###-###-#### (Office)###-###-#### (Cell)Email | ***Add or delete rows as needed….*** |

***Definitions:***

***Primary Security Contact: This should be the person in the organization who oversees physical security for the applicable Development(s)***.

***Secondary Security Contact: This should be the person in the organization who oversees cyber security for the applicable Development(s) OR the person in the organization who is next in line for security related matters for the applicable Development(s)***.

***Alternate Contact: This should be for people who want to be in the know for security matters pertaining to the applicable Development(s), but not necessarily have a background in security (i.e. CDSE, VP of Hydro Operations, etc.) OR additional security members that the primary security contact wants on the security communication list. \*\*\*\*You may have up to three Alternate contacts, just create more rows in the table and label accordingly (i.e. Alternate Contact 1, Alternate Contact 2, etc.)\*\*\****