**Partners**

*5555 Turbine St*

*Atlanta, GA 99999*

*999-999-9999*

**December 31, 2020**

FERC-OEP Division of Dam Safety and Inspections

Attn: Mr. Wayne King, P.E.

Regional Engineer  
Atlanta Regional Office

Gwinnett Commerce Center

3700 Crestwood Pkwy NW, Suite 950

Duluth, GA 30096

Re: 2020 FERC D2SI Security Compliance Certification for: Orange Lake, P-09999-01; Boulder Falls, P-09999-02; Victoria Valley, P-09999-07; and Kale Pass, P-09999-08

Mr. King:

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.
* Cyber Security for the applicable above referenced Development(s) and those interconnected were reviewed/evaluated as detailed in Attachment 2-Cyber Asset Designation Sheet.
* 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.

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

Sincerely,

***Signature***

***Anthony DeLuca***

***Director of Hydro Operations***

***New Dominion Energy Partners***

***5555 Turbine St***

***Atlanta, GA 99999***

***999-999-9999***

***DeLucaA@NDEP.com***

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |
| Orange Lake | 09999-01 | 2 | 11/30/2020 | 11/30/2020 | NA | 06/01/2018\* | NA | NA | 09/15/2020 | 05/08/2012 |
| Boulder Falls | 09999-02 | 1 | 11/15/2020 | 11/10/2020 | 11/10/2020 | 07/29/2019 | 10/16/2020 | 05/18/2016 | 10/17/2020 | NA |
| Victoria Valley | 09999-07 | 3 | 11/30/2020\* | NA | NA | 06/25/2016\* | NA | NA | NA | NA |
| Kale Pass\* | 09999-08\* | 3\* | 11/30/2020\* | NA | NA | 06/25/2016\* | NA | NA | NA | NA |

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** |
| Orange Lake | | 09999-01 | 2 | 11/30/2020 | spillway gates | Operational | No |  | Complete; 10/15/2020 | 6 of 6 spillway gates remotely operated; PAR 0-3 <50 |
| Orange Lake | | 09999-01 | 2 | 11/30/2020 | powerhouse | Operational | Medium | 09/30/2020 | Complete; 10/15/2020 | 5 of 10 units remotely operated; Total Generation=150MW; Tailrace fishing activities immediately downstream of the powerhouse. BES Cyber System designated Medium impact under CIP-002-5.1a criteria - applying relevant security controls from CIP to this networked asset. |
| Orange Lake | | 09999-01 | 2 | 11/30/2020 | powerhouse | Non-critical | No |  | Complete; 10/15/2020 | 5 of 10 units locally operated. |
| Boulder Falls | | 09999-02 | 1 | 11/30/2020 | spillway gates | Critical | No |  | Complete; 11/30/2019 | PAR 0-3 > 250; 5 of 8 spillway gates are remotely operated. |
| Boulder Falls | | 09999-02 | 1 | 11/30/2020 | spillway gates | Non-Critical | No |  | Complete; 11/30/2019 | 3 of 8 spillway gates locally operated. |
| Boulder Falls | | 09999-02 | 1 | 11/30/2020 | powerhouse | Critical | Medium | 09/30/2020 | Complete; 11/30/2019 | 5 of 5 units remotely operated; Upstream water supply (disruption of essential services) and 3 hydroelectric projects. BES Cyber System designated Medium impact under CIP-002-5.1a criteria - applying relevant security controls from CIP to this networked asset. |
| Victoria Valley | | 09999-07 | 3 | 12/5/2020 | low-level outlet | Critical | Medium | 09/30/2020 | Complete; 11/30/2019 | Low-level outlet is non-critical assets by itself. Interconnected with Boulder Falls; adhere to the most critical connected cyber assets requirements. Protected as a CIP Medium Impact due to interconnection to Boulder Falls Powerhouse. |
|  |

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.: 09999-01 Proj/Dev Name: Orange Lake Licensee: *New Dominion Energy Partners***

**Security Group: 2 Date: 11/30/2020 Inspector/ Attendees: Todd Smith (Security Specialist); John Jones (CDSE)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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? | X |  | | Days/week 5 Hours/day 8 . | | | |
| Powerhouse? | X |  | | Days/week 5 Hours/day 8 . | | | |
| 2. Are there surveillance Dam?  cameras in use? | X |  | |  | | 2 PTZ cameras on dam crest, left and right abutment covering entire crest | |
| Powerhouse? | X |  | |  | | 1 fixed camera on northwest corner of powerhouse building to view main entrance door, 1 fixed camera on southwest corner of powerhouse to view rear access door | |
| Other? | X |  | |  | | 1 fixed camera on intake tower to view access gate | |
| How are they viewed/checked? | Cameras are viewed from the powerhouse control room on a separate monitor by operator during work hours. During after hours, cameras are viewed from the Energy Control Center (ECC) which is staffed 24/7. | | | | | | |
| 3. Is the frequency of walking inspections  appropriate (safety and/or security)? | X |  | |  | | Note the frequency of these inspections: Walking inspections are conducted once a week, every Mondays to check for weekend disturbances/activities. Perimeter and critical assets checked. | |
| Personnel control/ID badges used? |  | X | |  | | No card access technology at the development, however, employee IDs are kept on person | |
| **DELAY**  4. Is the dam site fenced with gates/doors  locked (if appropriate to the site)? | X |  | |  | | 7 Ft perimeter fencing and 1 ft 3 strand barbed wiring around each critical asset (dam, spillway, intake, and powerhouse). Vehicle gates are locked with chain and pad lock, all doors are locked and protected with latch guards. Locked at all times. | |
| 5. Is access restriction to the Foot?  dam/facilities appropriate  and in-place? |  | X | |  | | Majority of perimeter fencing is intact and with minimal gaps for intruder to gain access, however, erosion did occur underneath perimeter fence on the West side of powerhouse allowing for an intruder to crawl under – This will be addressed by December 31, 2020 | |
| Vehicle? | X |  | |  | | Chain-link vehicle gate – manually operated is locked with ½ inch cut resistant chain and lock. | |
| Boat? |  | X | |  | | No boat barrier in place – boat boom on reservoir solely used for demarcation. | |
| 6. Are spillway/gate controls secured  against unauthorized access? | X |  | |  | | Lockbox and padlocks on all spillway gate controls – power supply required to control gates. Power supply access in powerhouse. | |
| 7. Are powerhouse doors/  windows locked? | X |  | |  | | Both powerhouse exterior doors are locked with 6 pin locks to include deadbolts. Windows are 20 feet high and opened for airflow. Roof hatch locked from internal side | |
| Alarms/motion detection/cameras? | X |  | |  | | Specify details:  Both exterior powerhouse doors are protected with balanced magnetic switches (BMS) and are monitored by ECC during afterhours. Redundant monitoring is conducted by Intrusion Detection Inc. No motion detection or other detection capabilities exist. | |
| Can systems be easily bypassed? | X |  | |  | | Security systems critical assets other than powerhouse can be easily bypassed since no detection exists at those structures. | |
| 8. Water conveyance Access restricted?  system: | X |  | |  | | Perimeter fencing around intake tower – restricted area signs posted. However, very difficult to restrict access to overhead penstock due to the geography of layout. | |
| Surveillance? | X |  | |  | | 1 fixed camera on intake tower to view access gate, however no cameras to view penstock due to lack of communication capabilities in rural area. Periodic physical walkthrough/inspections conducted along penstock | |
| 9. Is critical performance monitoring  equipment secured against tampering? | X |  | |  | | All piezometers capped and locked. Instrumentation locked in junction boxes. | |
| **Field Observations** | **Y** | **N** | | **NA** | | **Comments** | |
| **RESPONSE**  10. Are law enforcement phone numbers  posted? | X |  | |  | | Any County Sheriff’s Offices for emergency and non-emergency phone numbers posted in control room, stored on speed dial on telephone and employee cell phones. | |
| 11. Are there redundant communications? | X |  | |  | | smart phones, 2-way radios, and land lines are redundant means of communication | |
| 12. How long it takes the operator if detected to respond to unauthorized access? | How is detection made? Detection at powerhouse is made through Intrusion Detection System (IDS). Powerhouse doors are protected with BMS – when the magnetic field is broken from a forced entry, an alarm notification will be sent to the control room, ECC, and Security vendor. Detection for all other critical assets cannot be achieved, unless visually detected at the time of an event. Operators live on site – response time is less than 5 minutes | | | | | | |
| What is that response? | Operator will make initial assessment – if urgent, immediately contact law enforcement to respond to incident. It the event is not urgent, operator will report to Supervisor to determine whether law enforcement is required, then write an internal report of incident for record keeping and trend tracking. | | | | | | |
| 13. Can law enforcement be quickly  notified? | X | |  | |  | | Identify enforcement agenc(ies): & capabilities: Any County Sheriff’s Office, Any County State Police – 20 deputies, 4 state police in area – if necessary, state will provide SWAT team |
| Estimated time for arrival? | Any County Sheriff’s Office – 10-20 minutes, State Police – 30-45 minutes | | | | | | |
| **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. | Threat Assessment conducted with Any County Sheriff’s Office on September 1, 2020. Social Media Environmental Group launched a campaign to remove the Orange Lake Dam for concerns of the salmon run. Threats were made to attack dam using explosive resources. The dam is an earth embankment dam with no freeboard. If compromised, 1,000 homes can be flooded. A moderate amount of resources can be acquired to break the dam. The Any County Sheriff’s Office was notified and is working in collaboration with the FBI to investigate the threat posted on social media. Our corporate security is also closely monitoring social media feeds and trends. So far, no arrests have been made.  Last time consultation with law enforcement was made to determine threat: | | | | | | |
| 15. Steps taken to improve Past year:  security: | Strengthened security operational procedures by increasing site inspections, stringent screening policy, increasing presence, increasing community outreach and relationships with law enforcement. Hired additional personnel solely responsible for monitoring/reporting suspicious activities. Developed in-house security awareness training, attend third party active shooter training, effective physical security training for dam, and joined sector council for security education and risk mitigation. | | | | | | |
| Long term plans: | Upgrade camera system/software to integrate with intrusion detection system. Install additional cameras with detection capabilities around powerhouse/dam and rec area | | | | | | |
| 16a. Is there a Security Plan  (Group 1 or 2) | X |  | |  | | If “Yes” is it acceptable? SP has been tested and is effective  Is there a Response/Recovery Plan component? Yes, Response only; effective | |
| Are there different site-specific  response levels covered in the  Security Plan for varying threat? | X |  | |  | | Summarize levels/activities: DHS NTAS – Normal, Elevated, Imminent Threat levels determines increase in security posture and procedures (e.g. contract guards, restrict public access, increase liaison with LE, vehicle screening, restrict deliveries and vendors/contractors, execute Incident Command System) | |
| Are the measures on the day of  inspection consistent with the  current threat level? | X |  | |  | | If “no” explain: Normal threat level – normal security operating procedures and measures in place. | |
| 16b. Has Security plan been revised since  last field change? | X |  | |  | | Updated screening procedures for new employees, updated security operational procedures, updated training policy/procedures, and updated contacts (revised 11/30/2020)  When it was last exercised & what type? June 1, 2018 – Tabletop in conjunction with EAP | |
| 17. Is there a Vulnerability Assessment?  (Group 1) |  |  | | X | | If “Yes” is it compliant? VA not required for Group 2 | |
| 18. Is there a Security Assessment?  (Group 1 or 2) | X |  | |  | | If “Yes” is it compliant? Yes, assessed security effectiveness against unarmed intruder with no specialized tools or weapons. Recommendations for improvement developed – September 15, 2020 | |
| 19. Are all actions and plans fully  integrated? |  | X | |  | | No 360-degree detection capabilities, minimal delay – recommendations for improvement developed – September 15, 2020 | |
| 20. Do any security measures conflict  with any license requirements? |  | X | | All recreation areas open to public, no known security concerns at this time. | | | |
| 21. Is there HAZMAT/fuel storage on-site? | X |  | | Describe: Diesel generator fuel, oil, and oxygen tanks stored in locked climate-controlled shed. | | | |
| If so, is access secured? | X |  | | Door lock and deadbolt on storage shed | | | |
| 22. Are critical drawings/plans/records  secured from unauthorized access? | X |  | |  | | Located in locked file cabinets in control room. Employees must get supervisor approval to access critical drawings/plans/records. Copy of SP also locked in cabinet. Digital copies stored in secured network drive at the ECC. | |
| 23. We have no comments about the  Security Measures observed: | X |  | | If no comments, check “No”; if comments needed, check “Yes”. Developing a plan and schedule to increase detection capabilities and delay features for integrated system | | | |
| If comments needed, follow-up  actions will be made and tracked | List potential remediation discussed: Install sensors/integrated with camera system, upgrade camera system software, install additional security cameras with detection capabilities around the development. | | | | | | |

**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.  1 | Description (indicate if it was it reported to FERC)  June 24, 2020 - Trespassing event on dam crest (restricted area) – hiker was lost – operator confronted hiker and hiker left the site. Event reported to FERC Regional Office |
| B. Owner expressed specific security concerns or questions. | Yes, Environmental Group potentially targeting dam. Law enforcement notified – investigation underway. |
| C. Number (description) of data requests or  site visits by DHS PSA or other  assessment groups. | None – Future plans to request PSA assessment |
| D. Changes made to security since last inspection: | Indicate “None” by checking here: .  Do previous studies show prior posture was adequate?(y/n) . Prior posture is inadequate due to lack of detection – plans for improvement are underway |
| Following changes were made  to physical site security: | If so, describe changes: Hired additional personnel solely responsible for monitoring/reporting suspicious activities. |
| Following changes made to  procedural operations (incl.  threat level increase additions,  employee actions, etc.): | If so, describe changes: Increased site inspections, stringent screening policy, increased presence, increasing community outreach and relationships with law enforcement. Developed in-house security awareness training, attend third party active shooter training, effective physical security training for dam, and joined sector council for security education and risk mitigation. |
| Following changes/additions  made to cyber/SCADA  operations: | If so, describe changes: Operational Cyber Asset (spillway gates 6 of 6; and powerhouse 5 of 10 units). Project is operated from our Hydro Center. Employees must utilize dual factor authentication to access SCADA data. Additional cyber-security measures are in place for the spillway gates as required by FERC and the powerhouse controls fall under NERC. |
| 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). Risk is fairly low, ASR value is currently at .124, Increasing detection capabilities in the near future will drive the risk down half to .062. |
| 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): X . Will not e-file and security related documents including the annual security compliance certification letter.  No, discussion was not made (reason why). |

**FERC SECURITY CHECKLIST (v5a)**

**Field Security Inspection Form 1**

**Project-Development No.: 09999-02 Proj/Dev Name: Boulder Falls Licensee: *New Dominion Energy Partners***

**Security Group: 1 Date: 11/30/2020 Inspector/ Attendees: Todd Smith (Security Specialist); John Jones (CDSE)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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? | X |  | | Days/week 5 Hours/day 8 . Note: Dam Tender lives on site | | | |
| Powerhouse? | X |  | | Days/week 7 Hours/day 24 . | | | |
| 2. Are there surveillance Dam?  cameras in use? | X |  | |  | | 4 PTZ cameras w/Video analytics on dam crest, left and right abutment, on both sides, covering entire crest (upstream/downstream) and spillway. 1 PTZ w/video analytics at main vehicle entry gate to dam off Hwy 999. 1PTZ w/video analytics on back road to dam Co. Rd 777 | |
| Powerhouse? | X |  | |  | | 4 PTZ cameras w/video analytics on each corner of powerhouse for 360-degree view of powerhouse access points. 1PTZ w/video analytics on guard post at gate entrance to cover incoming vehicles/persons. 4 internal PTZ cameras w/video analytics on each corner of generating floor. 1 fixed camera w/video analytics at control room door. 4 PTZ cameras w/video analytics in powerhouse lower-level | |
| Other? | X |  | |  | | 2 PTZ cameras w/video analytics on intake tower to view access gate, and boats approaching intake structure. 1 PTZ camera w/video analytics to view approaching persons/vehicles at outlets works. 3 PTZ cameras w/video analytics – one at boat launch, one at camp site check-in, one t visitor center/camp store. | |
| How are they viewed/checked? | Cameras are viewed and monitored from the main guard post at powerhouse 24/7. Redundant/back-up capabilities exists at Corporate Security Operations Center (SOC) which is staffed 24/7. Entire camera system is connected through fiber wire. Network Video Recorder (NVR) system installed. | | | | | | |
| 3. Is the frequency of walking inspections  appropriate (safety and/or security)? | X |  | |  | | Note the frequency of these inspections: Walking inspections are conducted once daily as part of security guard post orders. Minimum of 3 guards on post per shift. Third shift inspects development perimeter and all critical assets prior to relieving second shift. Second shift reports any findings/events to third shift prior to leaving. | |
| Personnel control/ID badges used? |  | X | |  | | HID key card ID/electronic access for all exterior doors and critical interior doors (e.g. control room) is utilized at the development. Employee/contracted guards are vetted prior to issuance. ID badges must always be worn/visible, on-site. | |
| **DELAY**  4. Is the dam site fenced with gates/doors  locked (if appropriate to the site)? | X |  | |  | | 8 ft wrought iron fence (anti-climb meshing) with concertina wire and signage around entire perimeter. 7 ft. chain linked fence with 1 ft V-shaped outriggers and concertina wire each critical asset (dam, spillway, intake, and powerhouse). Anti-ram vehicle gate (mechanical) at main entrance, motor housing locked and inside perimeter, guard post included. Locked at all times, access granted with ID badge. | |
| 5. Is access restriction to the Foot?  dam/facilities appropriate  and in-place? | X |  | |  | | Anti-climb meshing on perimeter fence with concertina wire. | |
| Vehicle? | X |  | |  | | Anti-ram vehicle gate rated for 15,000 lbs. at 40 mph at perimeter. Interior gates at critical assets locked with ½ inch cut resistant chain and pad lock. | |
| Boat? |  | X | |  | | No boat barrier in place – boat boom on reservoir solely used for demarcation. However, on-site guards exist and PTZ w/video analytics for detection is available. | |
| 6. Are spillway/gate controls secured  against unauthorized access? | X |  | |  | | No electronic gate controls at exterior – all electronic controls are completed through SCADA system inside the control room. Manual back-up controls require hoist system. Hoist is locked and power feed from powerhouse required, | |
| 7. Are powerhouse doors/  windows locked? | X |  | |  | | Card access control for 4 powerhouse exterior doors, locked with maglocks rated at 1,800 lbs. holding force. Windows are 20 feet high and opened for airflow – steel grating installed. | |
| Alarms/motion detection/cameras? | X |  | |  | | Specify details:  All exterior doors at critical assets are protected with balanced magnetic switches (BMS). Camera system can also detect any change in pattern at protected areas including exterior doors. Motion sensors are installed inside the powerhouse generating floor, lower level, and outside the control room at upper level. Alarms are monitored by on-site security guards and back-up at SOC. | |
| Can systems be easily bypassed? |  | X | |  | | 360-degree detection, assessment, delay, and response exists. As technology and on-site security guards provide effective physical security. | |
| 8. Water conveyance Access restricted?  system: | X |  | |  | | 7 ft. chain linked fence with 1 ft V-shaped outriggers and concertina wire at intake structure. Additionally, perimeter fencing is equipped with anti-climb mesh for added delay. Restricted area signs are also posted. | |
| Surveillance? | X |  | |  | | 2 PTZ cameras w/video analytics on intake tower to view access gate, and boats approaching intake structure. 1 PTZ camera w/video analytics to view approaching persons/vehicles at outlets works. | |
| 9. Is critical performance monitoring  equipment secured against tampering? | X |  | |  | | All piezometers capped and locked. Instrumentation locked in junction boxes. | |
| **Field Observations** | **Y** | **N** | | **NA** | | **Comments** | |
| **RESPONSE**  10. Are law enforcement phone numbers  posted? | X |  | |  | | Any County Sheriff’s Offices for emergency and non-emergency phone numbers posted in control room, stored on speed dial on telephone and employee cell phones. | |
| 11. Are there redundant communications? | X |  | |  | | smart phones, 2-way radios, land lines, and satellite phones are redundant means of communication | |
| 12. How long it takes the operator if detected to respond to unauthorized access? | How is detection made? Detection on occurs through video analytic system, motion sensors, BMS, and roving guards for all critical assets. | | | | | | |
| What is that response? | Immediate response from on-site armed guards when detections made. | | | | | | |
| 13. Can law enforcement be quickly  notified? | X | |  | |  | | Identify enforcement agenc(ies): & capabilities: Any City Police Department, Any County Sheriff’s Office, Any City Police Department – 30 officers, Any County Sheriff’s Office – 45 deputies, Any State Police – 10 Officers – Any City PD and Any County Sheriff’s Office both have SWAT team. 3 Park Rangers also available to respond. |
| Estimated time for arrival? | Any City PD 5-10 minutes, Any County Sheriff’s Office – 10-20 minutes, State Police – 20-30 minutes, Park Rangers – 5-10 minutes | | | | | | |
| **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. | Threat Assessment conducted with State Fusion Center on September 1, 2020. The Cyber Division indicated that hydroelectric projects in the area are being targeted as a movement in support of #Turnoffthelights. New Dominion Energy Partners have worked in collaboration with DHS CISA and the FBI Cyber Division to develop mitigating measures against cyber-attack to the ICS for Boulder Lake Dam. Based on the threat and generation capacity (potentially impact 100,000 customers), New Dominion has implemented additionally enhancements to increase the effectiveness of our cyber security program with expert guidance from federal agencies. The ISC is air gapped, black and white listing protocol are in place, enhanced detection software has been implemented, and we are closely monitoring all cyber activity in and out of our network. No physical treat is known at this current time. A follow-up consultation with CISA and the FBI is scheduled for December 1, 2020.  Last time consultation with law enforcement was made to determine threat: | | | | | | |
| 15. Steps taken to improve Past year:  security: | Upgraded camera system to include video analytics, installed fiberoptic wire, increased number of guards per shift – from unarmed to armed. Enhanced security operating procedures to include daily inspections from previous weekly inspections. | | | | | | |
| Long term plans: | Install additional cameras w/video analytics throughout perimeter. Install fence disturbance sensors on chain linked fence. Install card access on interior vehicle gates. | | | | | | |
| 16a. Is there a Security Plan  (Group 1 or 2) | X |  | |  | | If “Yes” is it acceptable? SP has been tested and is highly effective  Is there a Response/Recovery Plan component? Yes, effective, ICS, Internal Response and Rapid Recovery/Resiliency | |
| Are there different site-specific  response levels covered in the  Security Plan for varying threat? | X |  | |  | | Summarize levels/activities: DHS NTAS – Normal, Elevated, Imminent Threat levels determines increase in security posture and procedures (e.g. increase number of armed guards, contract with law enforcement, restrict public access, vehicle screening, restrict deliveries and vendors/contractors, execute Incident Command System) | |
| Are the measures on the day of  inspection consistent with the  current threat level? | X |  | |  | | If “no” explain: Normal threat level – normal security operating procedures and measures in place. | |
| 16b. Has Security plan been revised since  last field change? | X |  | |  | | Updated security operating procedures for daily inspections and guards, updated SP to reflect security enhancements, screening procedures for visitors, updated SOC contacts (11/15/2020)  When it was last exercised & what type? July 29, 2019 – Full Scale with Local and State PD – Active threat scenario starting at camp site, then moving to powerhouse. | |
| 17. Is there a Vulnerability Assessment?  (Group 1) | X |  | |  | | If “Yes” is it compliant? VA is compliant. 5DBTs assessed for each critical asset to capture consequence, vulnerability, and likelihood of attack. (updated 10/16/2020) | |
| 18. Is there a Security Assessment?  (Group 1 or 2) | X |  | |  | | If “Yes” is it compliant? Yes, assessed security effectiveness against 5DBTs. Recommendations for additional improvement developed – October 17, 2020 – plan and schedule for June 30, 2021 | |
| 19. Are all actions and plans fully  integrated? | X |  | |  | | Full 360-degree protection – Deter, Detect, Assess, Delay, Respond. | |
| 20. Do any security measures conflict  with any license requirements? |  | X | | All recreation areas open to public, no known security concerns at this time. | | | |
| 21. Is there HAZMAT/fuel storage on-site? | X |  | | Describe: Diesel generator fuel, oil, and oxygen tanks stored in locked climate-controlled shed. BMS on doors. | | | |
| If so, is access secured? | X |  | | Card reader access/maglock | | | |
| 22. Are critical drawings/plans/records  secured from unauthorized access? | X |  | |  | | Located in locked file cabinets in control room. Employees must get supervisor approval to access critical drawings/plans/records. Copy of SP also locked in cabinet. Digital copies stored in secured network drive at the Corporate Office. | |
| 23. We have no comments about the  Security Measures observed: |  | X | | If no comments, check “No”; if comments needed, check “Yes”. Security measures are effective, however additional improvements are planned | | | |
| If comments needed, follow-up  actions will be made and tracked | List potential remediation discussed: Install additional cameras w/video analytics, fence disturbance sensors at critical assets, card access at interior vehicle gates. | | | | | | |

**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.  2 | Description (indicate if it was it reported to FERC)  July 4, 2020 - Trespassing event on dam crest (restricted area) – Drunken boaters rode up to dam and attempted to get on crest – on-site security responded and removed them from dam site. Reported to FERC Atlanta Regional Office.  July 4, 2020 – One individual operating drone over dam and critical assets, law enforcement and FERC Atlanta Regional Office notified – images deleted. |
| B. Owner expressed specific security concerns or questions. | Yes, cyber threat targeting hydroelectric facilities. Collaboration with law enforcement – mitigation implemented. |
| C. Number (description) of data requests or  site visits by DHS PSA or other  assessment groups. 1 | Yes – DHS PSA assessment conducted April 15, 2019. Recommendations developed. |
| D. Changes made to security since last inspection: | Indicate “None” by checking here: .  Do previous studies show prior posture was adequate?(y/n) . Yes, adequate |
| Following changes were made  to physical site security: | If so, describe changes: Upgraded camera system (from DVR to NVR, installed fiberoptic) and software, installed anti-climb mesh, increased number of guards per shift. |
| Following changes made to  procedural operations (incl.  threat level increase additions,  employee actions, etc.): | If so, describe changes: Increased site inspections, Criminal background screening policy for visitors, temporary badge for contractors (deactivate/reactive daily only when working on site), increasing community outreach and relationships with law enforcement. Mandatory annual security awareness training, third party training for dams, attend conference, join sector coordinating council and InfraGard. |
| Following changes/additions  made to cyber/SCADA  operations: | If so, describe changes: Currently critical cyber asset due to remote operations. However, measures for critical cyber assets implemented with additional enhancements based on CISA and FBI recommendations. Enhanced detection/monitoring technology. Whitelist/blacklist software, air gapped network, dual factor authentication. Cyber security training for ICS (Idaho National Lab – DHS). Future plans to upgrade RTUs and PLCs. |
| 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). Risk is moderate, ASR value .426. Security enhancements reduce ASR to .185. |
| 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): X . Will not e-file and security related documents including the annual security compliance certification letter.  No, discussion was not made (reason why). |

Security related correspondence for the referenced Developments listed in Attachment 1-Security Documentation Table can be coordinated through:

|  |  |
| --- | --- |
| Primary Security Contact  Nadim Kaade  Director of Security  New Dominion Energy Partners  5555 Penstock St  Chicago, IL 99999  999-999-9999 (Office)  999-999-9999 (Cell)  KaadeN@NDEP.com | Secondary Security Contact  Solomon Karchefsky  Director of Cyber Security  New Dominion Energy Partners  5555 Forebay St  Washington, DC 99999  999-999-9999 (Office)  999-999-9999 (Cell)  KarchefskyS@NDEP.com |
| Alternate Contact 1  Anthony DeLuca  Director of Hydro Operations (CDSE)  New Dominion Energy Partners  5555 Turbine St  Atlanta, GA 99999  999-999-9999 (Office)  999-999-9999 (Cell)  DeLucaA@NDEP.com | Alternate Contact 2  Kenneth Earls  Deputy Director of Security  New Dominion Energy Partners  5555 Penstock St  Chicago, IL 99999  999-999-9999 (Office)  999-999-9999 (Cell)  EarlsK@NDEP.com |