**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 et. al.*

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 |
| Clear Springs | 09999-03 | 1 | 11/15/2020 | 11/10/2020 | 11/10/2020 | 08/20/2016 | 10/16/2020 | 05/18/2016 | 10/17/2020 | NA |
| Jones Dike | 09999-04 | 1 | 11/15/2020 | 11/10/2020 | 11/10/2020 | 07/29/2019 | 10/16/2020 | 05/18/2016 | 11/01/2020 | NA |
| Tacoma Narrows | 09999-05 | 2 | 11/30/2020 | 11/30/2020 | NA | NA | NA | NA | 08/15/2020 | 05/08/2012 |
| Blue Bluffs | 09999-06 | 2 | 11/30/2020 | 11/30/2020 | 11/30/2020\* | 06/25/2017\* | NA | NA | 09/11/2020 | 05/08/2012 |
| 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. |
| Clear Springs | | 09999-03 | 1 | 12/1/2020 | spillway gates | Critical | Low | 09/30/2020 | Complete; 01/30/2020 | Disruption of essential services; 4 of 4 spillway gates are remotely operated; PAR 0-3>60. Connected to the powerhouse, so CIP Low Impact designation applies (inherited from powerhouse). |
| Clear Springs | | 09999-03 | 1 | 12/1/2020 | powerhouse | Critical | Low | 09/30/2020 | Complete; 01/30/2020 | 6 of 6 units remotely operated; Powerhouse is NERC CIP Low Impact due to black start capability. Generation capacity <1500 MW, but disruption to essential services > municipal-wide. |
| Jones Dike | | 09999-04 | 1 | 12/2/2020 | powerhouse | Critical | Medium | 09/30/2020 | Complete; 11/30/2019 | Remote control capability to control Boulder Falls. Protected as a CIP Medium Impact due to interconnection to Boulder Falls Powerhouse. |
| Tacoma Narrows | | 09999-05 | 2 | 12/3/2020 | powerhouse | Operational | No |  | Complete, 05/30/2020 | 6 of 6 units remotely operated; Total output = 150 MW; railyard is disrupted for a meaningful period of time. |
| Blue Bluffs | | 09999-06 | 2 | 12/4/2020 | powerhouse | Operational | No |  | Complete; 12/30/2019 | 3 of 3 units remotely operated; Total Generation >100 MW |
| Blue Bluffs | | 09999-06 | 2 | 12/4/2020 | spillway gates | Non-critical | No |  | Complete; 12/30/2019 | 5 of 5 spillway gates; locally/manually operated |
| 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). |

**FERC SECURITY CHECKLIST (v5a)**

**Field Security Inspection Form 1**

**Project-Development No.: 09999-03 Proj/Dev Name: Clear Springs Licensee: *New Dominion Energy Partners***

**Security Group: 1 Date: 12/1/2020 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 4 Hours/day 10 . | | | |
| 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. 1PTZ off Hwy 312 to view vehicles driving down road to dam. 1PTZ video motion detection on back road to dam Co. Rd 773 | |
| Powerhouse? | X |  | |  | | 4 PTZ cameras w/video analytics on each corner of powerhouse roof for 360-degree view of powerhouse access points and perimeter. 1PTZ w/video analytics on light post at gate entrance to cover incoming vehicles/persons. 1 fixed camera at card reader to view personnel, contractors, and visitors accessing site. 6 internal PTZ cameras w/video analytics: (4) each corner of generating floor; (1) on north wall centered; (1) on south wall centered. 1 fixed camera w/video analytics at control room door. 1 fixed camera for battery room, 4 PTZ cameras w/video analytics in powerhouse lower-level, 2 PTZ with video analytics on roof, covering roof hatch and ladder well. | |
| 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, downstream side of dam. 1 PTZ w/video analytics at butterfly valve house. 3 PTZ cameras w/video analytics – one at boat launch, one at camp site check-in, one at visitor center/camp store. 1 PTZ with infrared for water treatment plant. BMS on all doors for powerhouse, intake control house, and butterfly valve control house. | |
| How are they viewed/checked? | Cameras are viewed and monitored from the guard shack inside 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. Digital Video Recorder (DVR) system installed. All cameras have infrared technology. Alarm notification sent to guard shack and SOC. | | | | | | |
| 3. Is the frequency of walking inspections  appropriate (safety and/or security)? | X |  | |  | | Note the frequency of these inspections: Walking inspections are conducted twice daily as part of security guard post orders. Minimum of 2 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 | |  | | 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 be worn/visible at all times, 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 30 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. County Sheriff’s Marine Patrol available | |
| 6. Are spillway/gate controls secured  against unauthorized access? | X |  | |  | | Electronic gate controls are protected with steel cover box and anti-tamper sensor. Remote/automated operations controlled in powerhouse 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 15 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 exist. 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. BMS on intake control house door. Additionally, perimeter fencing is equipped with anti-climb mesh for added delay. Restricted area signs are also posted. Butterfly valve house secured with mag lock (1,800 lbs – holding force) – card reader access. | |
| Surveillance? | X |  | |  | | 2 PTZ cameras w/video analytics on intake tower to view access gate, and boats approaching intake structure. County Sheriff’s Marine Patrol to surveil reservoir and respond to boats approaching intake. 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 with anti-tampered sensors. | |
| **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, text messaging, 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 occurs through video analytic system, motion sensors, BMS, Video Motion Detection, and roving guards for all critical assets. | | | | | | |
| What is that response? | Immediate response from on-site armed guards when detection is made. Marine patrol present for additional support during peak recreation season. | | | | | | |
| 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 – 20 officers, Any County Sheriff’s Office – 35 deputies, Any State Police – 7 Officers – Any City PD and Any County Sheriff’s Office both have SWAT team. County Sheriff’s Marine Patrol – 2 Deputies. ATVs also available |
| Estimated time for arrival? | Any City PD 5 minutes, Any County Sheriff’s Office – 10 minutes, State Police – 30 minutes, County Sheriff’s Marine Patrol – 3-5 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 and State Police on September 1, 2020. The threat assessment consists of known domestic terrorist group called Merciless Crusaders (MC) conducting modern warfare training near the dam. Intelligence suggest the domestic terrorist group are working closely with international terrorist to plot an attack at the dam site and nearby campground to attack soft targets and obtain as many casualties as possible. New Dominion Employees and recreators are vulnerable to small arms attack. Local law enforcement and the FBI are surveilling the training compound as investigations continue. New Dominion was advised to increase the threat level to elevated and have adjusted security posture accordingly until threat level decreases. Additional security guards have been deployed  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 and video motion detection, installed fiberoptic wire, increased number of guards per shift – from unarmed to armed for increased threat levels. Enhanced security operating procedures to include bi-daily inspections from previous daily inspections. Allowed access of video feed to County Sheriff’s Office | | | | | | |
| 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. Establish long-term contract with local law enforcement | | | | | | |
| 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 and Resiliency/Recovery | |
| 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 bi-daily inspections, updated SP to reflect security enhancements, screening procedures for visitors, contractors/vendors, updated SOC contacts, updated key control procedures, and updated post orders for contracted guard force. (updated 11/15/2020)  When it was last exercised & what type? August 20, 2016 – Functional Exercise with Local and State PD – WBIED on face of dam from upstream side. | |
| 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. (reviewed/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 March 31, 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. Propane tanks are covered behind concrete wall. | | | |
| 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, in ground vehicle (metal detectors) 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.  1 | Description (indicate if it was it reported to FERC)  September 30, 2020 – Photography of Dominion personnel movement at powerhouse. Photography of boaters and recreators in the area. Person of interest may be part of domestic terrorist group. Local LE, FBI and FERC were notified. |
| B. Owner expressed specific security concerns or questions. | Yes, domestic terrorist group planning to attack soft targets. Collaboration with law enforcement – increased security measures. |
| C. Number (description) of data requests or  site visits by DHS PSA or other  assessment groups. 1 | Yes – DHS PSA assessment conducted June 30, 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 to include video analytics and video motion detection, installed fiberoptic wire, increased number of guards per shift – from unarmed to armed for increased threat levels. Allowed access of video feed to County Sheriff’s Office |
| Following changes made to  procedural operations (incl.  threat level increase additions,  employee actions, etc.): | If so, describe changes: Increased site inspections to bi-daily inspections from previous daily inspections, Criminal background screening policy for visitors/vendors/contractors, prior notice for visitors, restrict public access indefinitely, temporary badge for contractors while working on site, increased relationships with law enforcement. Mandatory annual security awareness training |
| Following changes/additions  made to cyber/SCADA  operations: | If so, describe changes: Currently Critical cyber asset due to remote operations. Baseline and Enhanced measures implemented for critical cyber assets. Additional enhancements implmeneted based on CISA and FBI mitigation recommendations. Enhanced detection/monitoring technology. Tracking and reporting attempted intrusion. Whitelisting function, air gapped network, dual factor authentication. Cyber security training for ICS with Sandia Labs. CISA assessment conducted. |
| 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 .326. Security enhancements reduce ASR to .163. |
| 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.: 09999-04 Proj/Dev Name: Jones Dike Licensee: *New Dominion Energy Partners***

**Security Group: 1 Date: 12/2/2020 Inspector/ Attendees: Ben Matlock (Security Specialist); Indiana 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 7 Hours/day 24 . | | | |
| 2. Are there surveillance Dam?  cameras in use? | X |  | |  | | 3 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 Route 1. 1PTZ w/video analytics on back road to dam 1 Dam Rd. | |
| Powerhouse? | X |  | |  | | (6) 5MP fixed HD cameras w/video analytics on each corner of powerhouse for 360-degree view of powerhouse access points. (1) 2MP fixed HD camera w/video analytics on guard post at gate entrance to cover incoming vehicles/persons. (2) 2MP fixed HD cameras on each corner of generating floor. 1 fixed camera w/video analytics at control room door. 4 IR-capable HD 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 3 times daily as part of security guard post orders. Minimum of 3 guards on post per shift. Each shift performs a walking inspection as part of the shift change. 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 |  | |  | | Dual technology proximity ID card 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 be worn/visible at all times, on-site. | |
| **DELAY**  4. Is the dam site fenced with gates/doors  locked (if appropriate to the site)? | X |  | |  | | 7ft. chain linked fence w/1ft top guard at 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 top guard and established clear zones preventing easy access over the fence. | |
| Vehicle? | X |  | |  | | Anti-ram vehicle gate K-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. All Windows lower than 12 feet high have additional 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 exist. 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 |  | |  | | 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 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 the State Police and Fusion Center, consisted of incident and law enforcement reporting from October 1, 2019 to September 30, 2020, identifying the most credible and likely domestic threats in the project area of operations. An incident where the perimeter vehicle gate was accessed by protesters crawling under the bottom of the fence and manually opening the gate by accessing the unsecured gate controller box. Other protesters piggy-backed after a maintenance worker entered the inner perimeter vehicle gate. Once inside the perimeter, protesters attempted to access the dam crest to manually close spillway gates, but gate controls were secured. Law enforcement was notified and responded to remove protesters as they tried to access the dam crest and administration building, complaining of excessive water releases downstream flooding their crops. Gates with excess space at the bottom or between them are vulnerable to unauthorized persons who could access facilities or impact the operation of critical assets. Jones Dike employees have been given new vehicle access procedures and gate closing delay times have been decreased to prevent piggybacking. No cyber threat is known at this 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: July 12, 2020 | | | | | | |
| 15. Steps taken to improve Past year:  security: | Upgraded camera system to include video analytics, installed fiberoptic wire, and consider hiring contract guards. Ensure that all gate control boxes are secured. Enhance 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 and Resiliency/Recovery | |
| 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, updated SP to reflect security enhancements, screening procedures for visitors, updated SOC contacts (updated 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 – November 1, 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.  3 | Description (indicate if it was it reported to FERC)  July 12, 2020 – Local populace protesting excessive water releases downstream attempt to enter the administrative bldg (restricted area) w/o authorization.  Aug 14, 2020 – One individual operating drone over dam and critical assets, law enforcement and FERC Atlanta Regional Office notified – images deleted.  Sep 10, 2020 – Drunken boaters rode up to dam and attempted to get on crest. In this incident and the protests, on-site security responded and removed trespassers from dam site with the assistance of local police. Reported to FERC Atlanta Regional Office. |
| 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 any 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.: 09999-05 Proj/Dev Name: Tacoma Narrows Licensee: *New Dominion Energy Partners***

**Security Group: 2 Date: 12/3/2020 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 4 . | | | |
| Powerhouse? | X |  | | Days/week 5 Hours/day 8 . | | | |
| 2. Are there surveillance Dam?  cameras in use? | X |  | |  | | 1 PTZ camera on post at dam crest, right abutment covering entire crest. 1 PTZ on roof of gate control house to cover reservoir. 1 fixed camera inside gate control house to monitor PLC. 1 Fixed camera on post - downstream side at left abutment to cover tailrace/staff gauge (safety only – not security) | |
| 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 and substation. 1 fixed at powerhouse entrance gate to view approaching persons and vehicles. | |
| Other? | X |  | |  | | 1 fixed camera on intake tower to view access gate, 1 PTZ camera at substation. | |
| How are they viewed/checked? | Cameras are viewed from the powerhouse control room only on a separate monitor by operator during work hours. Chief Dam Safety Engineer also has access to camera system from Administration Building, however not monitored 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 month, at the beginning of the month. Operator walks perimeter for cut fence/damaged barbed wire. Cameras are inspected for cobwebs and serviceability. Any camera outages are reported to CCTV contractor ISeeU Technologies and repairs are made after Purchase Order approval. | |
| Personnel control/ID badges used? |  | X | |  | | No card access technology at the development, however, employee IDs are to be visible at all times | |
| **DELAY**  4. Is the dam site fenced with gates/doors  locked (if appropriate to the site)? | X |  | |  | | 7 Ft perimeter chain-linked fencing and 1 ft 3 strand barbed wiring around each critical asset (dam, spillway, intake, powerhouse and substation). However, the substation is a 7ft chain-linked with no top-guard due to existing perimeter fencing. Operator and utility company has keys to substation – procedures are in place for access to substation. 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, the back entrance to the dam is open – previous vehicle gate/perimeter fencing was removed due to damage from continuous winter storms allowing for an intruder to get on site by foot. Intruder must bypass rugged terrain on mountain side to access dam by foot. Plans are in place to mitigate open foot access. Request for proposals sent to security firms. | |
| 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. Boat boom removed in winter months. | |
| 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 gate control house which is locked and sensored. | |
| 7. Are powerhouse doors/  windows locked? | X |  | |  | | Both powerhouse exterior doors are locked with 6 pin locks to include deadbolts. Windows are 10 feet high and opened for airflow, only during summer months. Roof hatch locked from internal side, ladder well has a cover and is locked with padlock. | |
| Alarms/motion detection/cameras? | X |  | |  | | Specify details:  Both exterior powerhouse doors and gate control house are protected with balanced magnetic switches (BMS) and are monitored at the control room and Administration Building. During after hours, security contractor All Alarm Monitoring responds to alarms at development. Notification is sent to operator and Chief Dam Safety Engineer (CDSE). If none can be reached, then local law enforcement is notified and dispatched. | |
| Can systems be easily bypassed? | X |  | |  | | Security systems at critical assets other than powerhouse and gate control house can be easily bypassed since no detection exists at those structures. | |
| 8. Water conveyance Access restricted?  system: | X |  | |  | | Perimeter fencing with top guard around intake tower – restricted area signs posted. However, access can be made with boat and grappling hook. | |
| Surveillance? | X |  | |  | | 1 PTZ camera on intake tower to view access gate, and intake control building door. | |
| 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. | |
| 11. Are there redundant communications? | X |  | |  | | 2-way radios, land lines, and satellite phones are redundant means of communication – Poor cellular connectivity | |
| 12. How long it takes the operator if detected to respond to unauthorized access? | How is detection made? Detection at powerhouse and gate control house is made through Intrusion Detection System (IDS) by operator and CDSE during normal business hours. Powerhouse doors are protected with BMS. During after hours, All Alarm Monitoring detects and notifies New Dominion personnel and local law enforcement –Detection for all other critical assets cannot be achieved, unless visually detected at the time of an event. 2 Operators live 15 minutes from development – rotating on-call responsibilities. | | | | | | |
| 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 CDSE 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 – 5 deputies, Any State Police Department 2 state police in area – if necessary state will provide SWAT team |
| Estimated time for arrival? | Any County Sheriff’s Office – 30-45 minutes, State Police – 1 hour to 1.5 hours depending on current location | | | | | | |
| **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 May 1, 2020. No known credible threat has been observed/assessed. However, insider threat scenario was assessed based on previous incident at development with disgruntled employee. Insider has knowledge of project operations, access to critical assets, and motivation to sabotage critical features to cause downstream impacts. If all 10 spillway gates were open during hours of darkness, the potential to flood 100 homes immediately downstream of the dam is likely. Disgruntled employee/potential insider threat was forced to resign from the company and offered a severance package. The intent of the severance package is to prevent any intentional acts of sabotage against the company. Any County Sheriff’s Office was notified of past incident with disgruntled employee; however, no arrests have been made.  Last time consultation with law enforcement was made to determine threat: | | | | | | |
| 15. Steps taken to improve Past year:  security: | Develop plan to close back entrance of dam, improve security operational procedures by increasing site inspections, plan to install additional camera at back entrance of dam, and developed insider threat scenario training for personnel company wide. Conducted functional exercise on June 1, 2019 with Any County Sheriff’s Office and State Police to familiarize law enforcement personnel with development and it’s access points. Agreement has been made to conduct annual exercises with law enforcement. Contract with security consultant to re-write an effective security plan and conduct security surveys/assessments to measure current state of security. | | | | | | |
| Long term plans: | Upgrade camera system/software to integrate with intrusion detection system. Install additional cameras with detection capabilities around powerhouse, substation and back entry of dam, install adequate vehicle gate/fencing on back entry of dam reliable to withstand snow storms. | | | | | | |
| 16a. Is there a Security Plan  (Group 1 or 2) | X |  | |  | | If “Yes” is it acceptable? SP has been revised, but not tested  Is there a Response/Recovery Plan component? Yes, Incident Command System in place | |
| 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, contract with off-duty law enforcement, restrict public access, increase liaison with LE, increase walking inspections, conduct 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, periodic drug screening, increased inspection frequency, enhanced key control procedures, and updated contacts (updated 11/30/2020)  When it was last exercised & what type? Not required for SG2 | |
| 17. Is there a Vulnerability Assessment?  (Group 1) |  |  | | X | | If “Yes” is it compliant? VA not required for Group 2, however future plans to conduct full VA | |
| 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 – updated August 15, 2019 | |
| 19. Are all actions and plans fully  integrated? |  | X | |  | | No 360-degree detection capabilities, minimal delay – recommendations for improvement developed – updated August 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 and oxygen tanks stored in powerhouse lower level | | | |
| If so, is access secured? | X |  | | Door locks and BMS in powerhouse | | | |
| 22. Are critical drawings/plans/records  secured from unauthorized access? | X |  | |  | | Locked in file cabinets in control room. Employees must get supervisor approval to access critical drawings/plans/records. Copy of SP also locked in cabinet. Additional hard copies and digital copies stored in Administration Building – CDSE grants access. | |
| 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, delay features, and adequate response for integrated system. (response time is concern) | | | |
| If comments needed, follow-up  actions will be made and tracked | List potential remediation discussed: Install gate at back entry, upgrade camera system software, update current cameras and install additional security cameras with detection capabilities around the development, hire off-duty law enforcement. | | | | | | |

**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)  March 24, 2019 – Disgruntled employee made verbal threats to co-worker of sabotaging dam and its critical assets. Co-worker reported to CDSE, CDSE reported to HR. Employee was removed with severance package. Local law enforcement and FERC Regional Office was notified. |
| B. Owner expressed specific security concerns or questions. | Yes, insider threat incident. Disgruntled employee may return to development and cause harm |
| 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 and delay– plans for improvement are underway – |
| Following changes were made  to physical site security: | If so, describe changes: New security plan and assessments will be finalized in 2020. Insider threat program/training developed |
| Following changes made to  procedural operations (incl.  threat level increase additions,  employee actions, etc.): | If so, describe changes: Increased site inspections, stringent employee screening policy, increased relationships with law enforcement. Developed 3rd party Insider threat training program and in-house security awareness training, increased key control procedures, and joined sector council for security education and risk mitigation. |
| Following changes/additions  made to cyber/SCADA  operations: | If so, describe changes: Currently Operational 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 fairly low, ASR value is currently at .114, Increasing detection capabilities and adequate delay in the near future will mitigate the risk to .057. |
| 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.: 09999-06 Proj/Dev Name: Blue Bluffs Licensee: *New Dominion Energy Partners***

**Security Group: 2 Date: 12/4/2020 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 12 . | | | |
| Powerhouse? | X |  | | Days/week 5 Hours/day 12 . | | | |
| 2. Are there surveillance Dam?  cameras in use? | X |  | |  | | 2 PTZ cameras on dam crest, left and right abutment covering entire crest and associated vehicle access points. | |
| Powerhouse? | X |  | |  | | 1 fixed camera on northwest corner of powerhouse building to view main entrance door, 1 fixed camera on the vehicle gate into powerhouse parking area to monitor vehicles and personnel coming in and out. | |
| Other? | X |  | |  | | 1 PTZ camera at Lunker Beach (FERC approved recreation area utilized by the public to launch boats, fish and picnic) | |
| How are they viewed/checked? | Cameras are viewed from the powerhouse control room on a separate monitor by the operator during work hours. During after hours, cameras are viewed from the Blue Bluffs City Operations Center (COC) 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 Monday to check for weekend disturbances/activities. Perimeter and critical assets are inspected. | |
| Personnel control/ID badges used? | X |  | |  | | No electronic access control system at the development, however, employee IDs are kept on person and required to be worn visible at all times. | |
| **DELAY**  4. Is the dam site fenced with gates/doors  locked (if appropriate to the site)? | X |  | |  | | 7-foot perimeter fencing with 1 foot 3 strand barbed-wiring top guard 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. Doors are locked at all times. | |
| 5. Is access restriction to the Foot?  dam/facilities appropriate  and in-place? | X |  | |  | | The perimeter fencing is intact and with no gaps for an intruder to gain access. A 10-foot wide clear zone is maintained on the inside and outside of the fence, it is kept clear of obstacles, topographical features, and vegetation. | |
| Vehicle? | X |  | |  | | Chain-link vehicle gates are at both sides of the dam crest and entrance into the secure powerhouse perimeter – they’re manually operated and locked with ½ inch cut resistant chain and lock. | |
| Boat? |  | X | |  | | No boat barrier or boom in place for the reservoir due to state regulations. | |
| 6. Are spillway/gate controls secured  against unauthorized access? | X |  | |  | | Lockbox and padlocks on all spillway gate controls – spillway gates can only be operated manually at each individual gate and its’ associated motor. | |
| 7. Are powerhouse doors/  windows locked? | X |  | |  | | Both powerhouse exterior doors are locked with 6 pin locks to include deadbolts. There are operable ground floor windows, however they all have locking mechanisms and cannot be opened from the outside. They also have high security steel grating installed on them. | |
| Alarms/motion detection/cameras? | X |  | |  | | Specify details: The powerhouse exterior doors have an Intrusion Detection System (IDS) installed. The IDS consist of balanced magnetic switches (BMS) mounted on both exterior doors and are monitored by COC during afterhours. | |
| 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 signage is in place. | |
| Surveillance? | X |  | |  | | The intake tower can be viewed by either of the 2 PTZ cameras located on the crest. | |
| 9. Is critical performance monitoring  equipment secured against tampering? | X |  | |  | | All piezometers are capped and locked. Instrumentation locked in junction boxes. | |
| **Field Observations** | **Y** | **N** | | **NA** | | **Comments** | |
| **RESPONSE**  10. Are law enforcement phone numbers  posted? | X |  | |  | | Blue City Police Department emergency and non-emergency numbers are posted in the control room next to the operator’s phone, they’re also stored as a favorite in all employee cell phones. | |
| 11. Are there redundant communications? | X |  | |  | | Cell 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 and the COC. Detection for all other critical assets cannot be achieved, unless visually detected at the time of an event. Operators can be on the site within 20 minutes. | | | | | | |
| What is that response? | Operator will make initial assessment – if urgent immediately contact law enforcement to respond to incident. It the event it’s 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: Blue City Police Department, Any County State Police – 39 officers, 9 state police in area – if necessary, city will provide SWAT team |
| Estimated time for arrival? | City Police Department – 10-15 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 by 007 Security Services, an independent security consultant, on August 31, 2020. The security consultant coordinated with local law enforcement to determine the majority of crimes in the area are break-in and theft. Law Enforcement stated intruders are stealing a lot of copper and scrap metals from local businesses to have money to buy drugs.  Last time consultation with law enforcement was made to determine threat: October 31, 2020 | | | | | | |
| 15. Steps taken to improve Past year:  security: | Replaced existing security cameras with newer IP based cameras with higher resolution and IR filters. Strengthened security operational procedures by increasing site inspections. Developed in-house security awareness training, attended third party active assailant training, and joined sector council for security education and risk mitigation. | | | | | | |
| Long term plans: | Upgrade camera system/software to integrate with intrusion detection system and activate/utilize the built-in video analytic capabilities of the new cameras. | | | | | | |
| 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, effective for both Response/Recovery Plan component | |
| 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 and updated the Physical Security Description/Inventory and Layout sections with the newer cameras. (updated 11/30/2020)  When it was last exercised & what type? June 25, 2017 – 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 – 5/8/2012; updated 9/11/2020 | |
| 19. Are all actions and plans fully  integrated? |  | X | |  | | No 360 degree detection capabilities, minimal delay – recommendations for improvement developed – September 11, 2020 | |
| 20. Do any security measures conflict  with any license requirements? |  | X | | All recreation areas are open to the 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 located outside inside a lattice fence for concealment purposes. | | | |
| If so, is access secured? |  | X | | Not specifically secured, but it is located within the perimeter fencing of the project. | | | |
| 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. | |
| 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 the 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)  Incident on March 21, 2020 – Trespassing/Theft incident at dam maintenance shop (restricted area) – maintenance shop was broken into and 101 feet of copper wire was taken. Event reported to FERC Regional Office and local law enforcement. |
| B. Owner expressed specific security concerns or questions. | Copper Theft Mitigation best practices and recommendations. |
| C. Number (description) of data requests or  site visits by DHS PSA or other  assessment groups. | DHS PSA performed a site visit on August 18th, 2020. Recommended that the old analog cameras be updated with IP based cameras with Infrared capabilities. PSA Recommendations were accepted and implemented. |
| D. Changes made to security since last inspection: | Indicate “None” by checking here: .  Do previous studies show prior posture was adequate?(y/n) 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: Replaced existing security cameras with newer IP based cameras with higher resolution and IR filters. |
| Following changes made to  procedural operations (incl.  threat level increase additions,  employee actions, etc.): | If so, describe changes: Strengthened security operational procedures by increasing site inspections. Developed in-house security awareness training, attended third party active assailant training, and joined sector council for security education and risk mitigation. |
| Following changes/additions  made to cyber/SCADA  operations: | If so, describe changes: Currently Operational cyber asset due to remote operations. Baseline cyber security measures implemented. Additional enhancements based on CISA and FBI notifications/recommendations. Third party cyber security assessment scheduled for March 2021. |
| 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 .130, Increasing detection capabilities in the near future will drive the risk down half to .071. |
| 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:

Security Contacts for Specific Development Numbers 09999-01, 09999-02, and 09999-03:

|  |  |
| --- | --- |
| Primary Security Contact  Nadim Kaade  Director of Security, East Region  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 |  |

Security Contacts for Specific Development Numbers 09999-04, 09999-05, 09999-06, 09999-07, and 09999-08:

|  |  |
| --- | --- |
| Primary Security Contact  Allen Frenette  Director of Security, West Region  New Dominion Energy Partners, LP  5555 Penstock St  San Fran, CA 99999  999-999-9999 (Office)  999-999-9999 (Cell)  FrenetteA@NDEP.com | Secondary Security Contact  Solomon Karchefsky  Director of Cyber Security  New Dominion Energy Partners, LP  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 |  |