NORTH SENECA
SOLAR PROJECT

APPENDIX 6-A

Site Security Plan

ORES Permit Application No. 23-00036

REVISION 1

SITE SECURITY PLAN

North Seneca Solar Project

Towns of Junius and Waterloo, Seneca County, New York

ORES Permit Application No. 23-00036

Prepared for:

NORTH SENECA
SOLAR PROJECT

North Seneca Solar Project, LLC
www.NorthSenecaSolarProject.com

Prepared by:

Environmental Design & Research, D.P.C.
217 Montgomery Street, Suite 1100
Syracuse, New York 13202
www.edrdpc.com

November 2024

TABLE OF CONTENTS

LIST OF ATTACHMENTS

1.0 INTRODUCTION

1.1 PROJECT DESCRIPTION

North Seneca Solar Project, LLC (the Applicant) proposes to construct the North Seneca Solar Project, an up to 90-megawatt solar energy generating facility located within the towns of Waterloo and Junius, Seneca County, New York (the Facility). The Facility Site will be located on private lands that are primarily rural in nature and will encompass approximately 940 acres, of which approximately 390 acres will be occupied by Facility infrastructure.

1.2 PURPOSE

The Applicant has developed this Site Security Plan (the Plan) in accordance with Title 16 New York Codes, Rules, and Regulations (16 NYCRR) Section 1100-2. 7(b) to identify the site-specific requirements to create and maintain a secure Facility Site during operation. Security is a critical component of any major electric generating facility. The purpose of the Plan is to ensure the secure and safe operation of the Facility through implementing physical and digital security measures, minimizing unauthorized access to the Facility, and protecting the equipment and components of the Facility from vandalism, theft, and damage. Site security features, including the approximate location of perimeter fencing and gates, are demonstrated in the Site Plan Drawings (see Appendix 5-A of the Article VIII Application).

2.0 SCOPE

The provisions of this Plan are mandatory for all site personnel, contractors, and visitors of the Facility.

3.0 RESPONSIBILITIES

It is anticipated that the Applicant will own and operate the Facility, except for the Point of Interconnection (POI) substation, which will be owned and operated by National Grid. Therefore, the Applicant anticipates being responsible for site safety and security during operation of the Facility, excluding the POI substation.

3.1 Site Manager

The manager of the Facility during its operational period (the Site Manager) will be responsible for the Plan's implementation and ongoing compliance. The Site Manager is responsible for the following:

- Ensure and verify compliance with this Site Security Plan, applicable federal, state, and local laws and regulations, as well as Certificate Conditions imposed by the Office of Renewable Energy Siting and Electric Transmission (ORES).
- Ensure that site personnel receive adequate training, resources, and support to comply with this Plan.
- Ensure that site personnel, contractors, and visitors adhere to this Plan.

- Document and report all security incidents to the Applicant.
- Conduct regular tests of the Cyber Security Incident Response Plan, at least once every 36 calendar months.
- Ensure compliance for all Transient Cyber Assets and Removable Media in accordance with the Facility's Transient Cyber Asset and Removable Media Plan.

3.2 Site Personnel and Contractors

All site personnel and contractors at the Facility Site will:

- Adhere to this Plan; and
- Report all security incidents to their supervisor or the Site Manager.

3.3 Applicant

The Applicant will be responsible for the following:

- Support the Site Manager's enforcement of this Plan;
- Conduct investigations of security incidents and take remedial actions including evaluation of increased security control measures as indicated in this Plan;
- Identify a Critical Infrastructure Protection (CIP) Senior Manager who will review and approve the Applicant's North Electric Reliability Corporation (NERC) CIP policies and procedures, and establish a process for delegating such authority (if delegations are used);
- Initially develop the Applicant's NERC CIP policies and procedures and periodically review them in accordance with the Applicant's Internal Compliance Program (ICP) for ongoing NERC compliance management;
- Periodically update this Plan to ensure compliance with the Applicant's NERC CIP policies and procedures, including the approval of any changes to this Plan by the CIP Senior Manager or delegate thereof;
- Implement processes to identify and categorize the Bulk Electric System (BES) Cyber Systems and associated Cyber Assets of the Facility (including periodic reviews thereof to be approved by the Applicant's CIP Senior Manager or delegate thereof) as defined in the requirements of the NERC CIP reliability standards;
- Develop and implement strategies to mitigate security risks, including the application of appropriate organizational, operational, and procedural security controls;
- Develop, implement, and regularly update a Cyber Security Incident Response Plan for the Facility in accordance with the Applicant's NERC CIP policies and procedures; and
- Develop, implement, and regularly update a Transient Cyber Asset and Removable Media Plan for the Facility in accordance with the Applicant's NERC CIP policies and procedures.

4.0 PHYSICAL SECURITY CONTROLS

4.1 Facility Access Gates

All entrances to the Facility from public roads will be gated to restrict access to the public. Signage at the entrances will be installed on gates warning the public not to trespass and of possible hazards in accordance with all federal, state, and local requirements. If unauthorized access and/or vandalism is found to be a reoccurring problem or gates are found to be damaged, security cameras will be evaluated for installation where necessary.

Gated access points to PV arrays and associated equipment, as well as to the collection substation, will be closed and locked except when authorized site personnel are working in and/or around these areas. Gates will be required to be kept locked when maintenance activities are not occurring. Violations of access road gate locking by contractors and visitors may result in them being banned from the Facility.

Emergency responders will be notified in the event of an unauthorized access emergency. A key box, known to first responders, will be installed at gated access points to permit access into the Facility in the event of an emergency.

4.2 Perimeter Fencing

Facility equipment, including photovoltaic (PV) arrays will be fully enclosed by gated security perimeter fencing to ensure public safety by deterring unauthorized access.

Signage will be posted on perimeter fencing stating it is a federal offense to damage property at an energy-generating facility and that no trespassing is allowed. If vandalism or trespass become an issue, alarm systems and/or surveillance cameras may be evaluated for use by the Applicant.

4.3 Collection Substation

The collection substation, located within the Facility Site, will also be fully enclosed with a chain-link security perimeter fence topped with three strands of barbed wire that extend 1 foot above the fence in accordance with the requirements of the National Electrical Code (NEC). The doors of the control building within the collection substation area will be kept locked unless site personnel are working in this location.

4.4 Field Enclosures

Field enclosures within the Facility perimeter fence may contain energized electrical equipment or other related solar equipment including network devices, data acquisition and control systems, and other programmable electronic devices and as such the field enclosures will remain locked at all times unless site personnel are working inside the enclosure.

4.5 Storage Trailer

A storage trailer will be located within the Facility Site to house the necessary tools, equipment, and spare parts required to conduct routine maintenance of the Facility.

The storage trailer will be locked when unoccupied and access will be granted only to authorized personnel. Should unauthorized access, vandalism, or damage occur to the storage trailer, additional intrusion detection methods will be evaluated by the Applicant.

5.0 ELECTRONIC ACCESS CONTROLS

5.1 Electronic Access Controls for Communications

Electronic access controls such as access control lists and firewalls/security gateways, will be implemented and maintained to permit only necessary inbound and outbound electronic access for any communications that are:

- Between a Facility BES Cyber System(s) and a BES Cyber Asset(s) outside of the Facility BES Cyber System;
- Using routable protocols when entering or leaving the Facility; and
- Not being used for time-sensitive protection or control functions between intelligent electronic devices.

5.2 Electronic Access Control Systems for Physical Access

Electronic access control systems, such as closed-circuit television (CCTV) video surveillance systems, gate entrance keypads, touchpad entry to buildings, and key management systems, are not proposed at the Facility at this time. Should unauthorized access, vandalism, or trespass become an issue, electronic access control systems will be evaluated by the Applicant.

6.0 CYBER SECURITY

The Applicant will ensure that the Facility is compliant with all applicable cyber security requirements. Savion has created company-wide cyber security procedures that are intended to provide a framework for the subsequent development of project-specific plans once facilities become operational. Note that these procedures are meant to be representative of the Applicant's commitment and may be modified in the future at the corporate level as well as at the Facility level. The applicable procedural documents are provided in Attachments A and B of this document. Attachment A addresses NERC Standard CIP-002-5.1a, "Cyber Security – BES Cyber System Categorization" and identifies and categorizes BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Attachment B provides written guidance to maintain compliance with Reliability Standard CIP-003. The standard requires the identification of a CIP Senior

Manager, documentation regarding the delegation of CIP authority, periodic review and approval of Cyber Security Policies, implementation of documented Cyber Security Plans, and declaring and responding to CIP Exceptional Circumstances. General components of the Facility-specific plan are outlined in sections below.

6.1 Cyber Security Awareness

The Site Manager will make the necessary provisions to provide the site personnel with regular (at least every 15 months) cyber security awareness training to reinforce proper cyber security practices including associated physical security practices.

6.2 Cyber Security Monitoring

The Applicant will ensure that the Facility has a 24-hour, 365 days per year monitoring and alerting system for all digital computer and communication systems and networks that support the Facility. This Facility will demonstrate compliance with current NERC CIP standards and will be secured using industry standard access restriction protocols. In addition to the monitoring and alerting system, the Applicant will keep an inventory of cyber assets at the Facility.

Multi-point tiered threat detection will be employed, and cyber monitoring will include all BES Cyber Assets at the site.

A Cyber Security Program compliance review will be performed by an independent auditor every six years in compliance with 16 NYCRR Section 1100-2.7(b)(5).

6.3 Cyber Security Incident Response

The Applicant will develop a plan for the Facility to manage the response to Cyber Security Incidents (a Cyber Security Incident Response Plan) in accordance with the Applicant's NERC CIP policies and procedures. The Site Manager will conduct regular tests of the Facility's Cyber Security Incident Response Plan at least once every 36 calendar months.

Cyber Security incidents (potential or actual) identified by the Cyber Security Monitoring partner, site personnel, or otherwise will be handled in accordance with the Facility's Cyber Security Incident Response Plan.

6.4 Transient Cyber Assets and Removable Media

The Applicant will develop a plan to manage the risks associated with malicious code that could be introduced to the Facility's BES Cyber Systems through the use of Transient Cyber Assets, such as laptops, cellular phones, or other wired and wireless devices, and Removable Media, such as USB storage devices ("thumb drives") and network attached storage devices (the Transient Cyber Asset and Removable Media Plan).

The Site Manager will be responsible to ensure all Transient Cyber Assets and Removable Media brought into the Facility are in compliance with the Transient Cyber Asset and Removable Media Plan.

7.0 SECURITY LIGHTING

This Plan details the anticipated security lighting that will be implemented at the Facility to maintain adequate security. Permanent security lighting will be installed at the collection substation as needed and required by applicable state and local standards. The lights installed will be automatic or manual as deemed necessary to minimize environmental and community impacts. Checking security lighting functionality will be a component of all maintenance inspections and any security lighting that fails will be promptly replaced. Additional information regarding security lighting of the proposed Facility can be found in the Lighting Plan (see Appendix 5-B - Revision 1 of the Article VIII Application) and the Visual Impacts Minimization and Mitigation Plan (see Appendix 8-B – Revision 1).

7.1 PV Array Lighting

PV arrays are not anticipated to include permanent lighting.

7.2 Collection Substation Lighting

Collection substation lights will meet the minimum requirements for security and maintenance safety to reduce light trespass to the surrounding environment. Lighting will be hooded downward and the lighting to be used will be of a wildlife-friendly, low-intensity wavelength (greater than 560 nanometers). The lighting will be placed on an automatic timer or light sensor set to turn off during daylight hours. Lighting at these components may be replaced with low-light video and/or camera surveillance monitoring or other security methods that do not require lighting, whenever practicable and as deemed necessary.

7.3 Lighting for Aircraft Safety

Lighting for aircraft safety is not required for the Facility, as the Facility does not include the installation of any components greater than 200 feet in height. Therefore, aircraft obstruction lighting is not applicable or required.