CORDELIO POWER

FLAT CREEK SOLAR

Permit Application No. 23-00054

Appendix 6-1

Site Security Plan

August 2024

Contents

Tables

Appendices

Site Security Plan

6(a) Introduction

Flat Creek Solar NY LLC (the Applicant) is proposing to construct Flat Creek Solar (Facility), a 300 megawatt (MW) photovoltaic (PV) solar energy generation facility in the Towns of Root and Canajoharie, Montgomery County, New York. The Facility is being permitted under Article VIII of the New York State Public Service Law. A schematic of the Facility and its major components is included in Appendix A, Facility Overview for Emergency Response. This Site Security Plan (SSP) describes security measures in place to ensure the safety and security of the Facility and its employees. These measures will prevent and minimize unauthorized access to the Facility and its infrastructure, thereby protecting Facility operations and the safety of the public. The SSP will be updated as warranted and will be enforced among all Facility employees and contractors. As required by 16 NYCRR §1100-2.7(d), the Applicant has provided copies of the SRP for review and comment to the New York State Division of Homeland Security and Emergency Services. At the time of the filing of the Article VIII Application, a response has not yet been received.

(1) Facility Overview

The Facility is a ground-mounted solar site proposed to be constructed in the Towns of Root and Canajoharie, Montgomery County, New York. The Facility will consist of solar arrays and associated infrastructure for the production of renewable energy, with a generating capacity of 300 megawatts. The Facility is anticipated to include single-axis tracker solar panels, power inverters to convert electricity from direct current (DC) to alternating current (AC), access roads, collection lines, a collection substation, and a Point of Interconnection (POI) switchyard to deliver electricity to the existing New York Power Authority (NYPA) 345 kV Transmission Line #352. The Facility will consist of the following components:

- Solar panel arrays;
- Inverters;
- Electric collection lines;
- Collection substation;
- Point of Interconnection (POI) switchyard; and
- Supporting infrastructure, including access roads and security fencing.

A schematic of the Facility and its major components is included in Appendix A, Facility Overview for Emergency Response.

6(b) Scope, Roles, and Responsibilities

The Facility may be unstaffed during operations and will be monitored remotely by Operations and Maintenance (O&M) staff. These internal and external staff will be collectively referred to as the O&M Service Providers. The Facility, including O&M Service Providers, will be managed and supervised by the Applicant's Facility Manager. Any threats to or violations of security should be reported to the Facility Manager or the Applicant. Table 1 below lists the roles and responsibilities of Facility personnel.

As noted above, the Facility may be unstaffed during normal operations. Facility operations will be monitored and controlled remotely around-the-clock, 365 days per year, by the Applicant's O&M Service Providers. Upon detection of concerns, the O&M Service Provider remotely monitoring the Facility will communicate with any Facility personnel who may be on-site and will dispatch O&M Service Providers to the Facility as needed.

On-site activities that require the presence of Facility personnel include routine maintenance, routine inspections, and unplanned maintenance. Routine inspections include examination of wiring, racking, and other equipment. Routine maintenance includes mowing, vegetation management, and stormwater control upkeep.

Table 1. Roles and Responsibilities of Facility Personnel

Role	Responsibilities
Facility Manager(s)	• Verify and enforce compliance with the Site Security Plan (SSP). • Verify and enforce compliance with applicable federal, State, and local laws. • Ensure that all Facility personnel receive appropriate training. • Oversee O&M Service Provider(s). • Coordinate with other Facility and/or Applicant representatives. • Assess potential security threats or violations and, if appropriate, contact the police. • Review and approve updates to the SSP.

Table 1. Roles and Responsibilities of Facility Personnel

Role	Responsibilities
	• Comply with SSP and SRP
Health, Safety, and Environmental Manager(s)	• Assign on-site Health, Safety, and Environmental responsibilities. • Ensure that the SSP is consistent with the Safety Response Plan (SRP). • Comply with SSP and SRP
On-Site Crew Leader(s)	• Ensure that on-site employees are registered for Facility access. • Ensure that on-site employees have read SSP and SRP. • Ensure that all employees exit the Facility upon work completion. • Ensure site security upon leaving the Facility. • Comply with SSP and SRP
Other Facility Personnel	• Report all security incidents to the On-Site Crew Leader or Facility Manager. • Comply with SSP and SRP

6(c) Site Security Measures

The following subsections outline the requirements for Site Security as outlined in §1100-2.7(b).

Efficient and reliable communication is crucial to ensure safe and secure Facility operations. It is expected that most Facility personnel will carry a personal or work-provided cell phone while working on-site. If deemed necessary, a two-way radio may be used between Facility personnel to quickly coordinate on-site activities. If on-site work involves multiple staff working in different areas of the Facility, then, at a minimum, each On-Site Crew Leader should carry a two-way radio and/or cell phone. Cell phones and radios should be in an audible ring mode while at the Facility. Should threats to safety or security arise, emergency services can be dialed from work-provided or personal cell phones. A list of local public safety agencies and emergency service providers is provided in Appendix B.

The O&M Service Providers are responsible for ensuring effective communication during on-site O&M activities. In the event of an emergency that threatens health, safety, or security, the Facility

Manager may contact local police. Incident reports and police reports will be filed by the Facility Manager.

(1) Access Controls

The Facility will comply with the following requirement outlined in §1100-6.4(i):

- All mechanical equipment will be enclosed by fencing of a minimum height of seven feet with a self-locking gate to prevent unauthorized access.

To ensure site security, the perimeter of the Facility will be enclosed by a security fence with several gates for personnel or emergency access. All equipment and photovoltaic solar arrays will be within permanently fenced areas. The perimeter fencing will be secured by self-locking gates to prevent unauthorized access into the Facility. Travel within the Facility will be facilitated by several access roads; within areas of Facility components, travel on these access roads will be restricted and will only be accessible after entering through a secured gate. Signs will be placed periodically along the perimeter fence and at each access point to deter trespassing. The signage will warn of trespassing, provide safety information, and provide contact details to report suspicious activity or request additional information. Local emergency responders will be provided access to all Facility entry points, via keys, knock boxes, or gate keypad codes; please see Appendix 6-2, Safety Response Plan, for additional information regarding safety and emergency procedures.

The Facility may be unstaffed during normal operations. The Facility will not be accessible to the public; all personnel must have authorization to enter the Facility. Visiting personnel should be approved by an O&M Service Provider or by the Facility Manager and must complete site access documentation. Visitors should be escorted through the Facility by authorized personnel unless otherwise authorized by the Facility Manager. All visitors requiring unescorted entry must be familiar with site security and safety requirements.

All Facility personnel and visitors are encouraged to report any signs of unauthorized entry or vulnerabilities to security, including fence breaches or unexpected damage to infrastructure. During on-site activities that require the presence of Facility personnel, such as construction, routine maintenance, routine inspections, or unplanned maintenance, On-Site Crew Leaders should tour their work areas daily to check security measures. Once reported, fence breaches and other security vulnerabilities will be repaired as soon as feasible.

(2) Electronic Security and Surveillance

Electronic security and surveillance measures will deter unauthorized Facility access and will alert the Applicant to security breaches. The Facility collection substation and POI switchyard will be equipped with motion-controlled lighting, entry alarms, and video surveillance capabilities. See Section 6(c)(3) below for a discussion of security lighting. O&M Service Providers will evaluate security threats and consider additional security measures to protect vulnerable areas.

(3) Security Lighting

Exterior Facility lighting will be limited to that which is required for health, safety, security, emergencies, and operational purposes and will be designed and installed to avoid off-site lighting effects. The Facility will not be lit during normal daytime operations. Motion-controlled lighting will be installed at the collection substation and POI switchyard to ensure site security during darkness. Additional motion-controlled lights may be added to vulnerable areas within the Facility, if deemed necessary. Streetlights, motion-controlled lights, photocell-activated lights, or manually operated lights may be installed at Facility access points, if deemed necessary for safety or security. Within the onsite collection substation and POI switchyard, manually operated task lighting will be installed in compliance with the National Electrical Safety Code; these lights will not be activated except during nighttime maintenance activities. Refer to the Facility Lighting Plan in Exhibit 5 (*Design Drawings*) of the Article VIII Application for additional detail regarding proposed Facility lighting.

In the rare case when Facility maintenance must occur during nighttime hours, temporary work lighting will be installed. Temporary nighttime work lighting will be limited to those areas undergoing maintenance and will be directed away from off-site facilities and residences as much as possible. Temporary work lighting will be shut down when not in use, unless required for safety and/or security purposes.

As the Facility does not involve components greater than 200 feet in height, the Facility will not compromise aircraft safety. Solar glare exposure will be avoided or minimized in accordance with the Visual Impact Minimization and Mitigation Plan (VIMMP) conducted for the Facility, provided within the Visual Impact Assessment (Appendix 8-1 of the Article VIII Application). The VIMMP includes an analysis of solar glare exposure to nearby airports, structures, and major roadways, as applicable.

6(d) Information and Cyber Security

(1) Information Security

To ensure information security, information systems will be secured using industry standard access restriction protocols.

(2) Cyber Security

To ensure cyber security, the data acquisition and supervisory control and data acquisition system (SCADA) will follow the North American Electric Reliability Corporation's (NERC) reliability standards. Cyber infrastructure will be stored in restricted-access areas. The Facility Manager will manage personnel access to cyber infrastructure. Rights to access cyber infrastructure will be routinely reviewed and modified by the Facility Manager or the Applicant's Information Technology Director. As required by 16 New York Codes, Rules, and Regulations (NYCRR) § 1100-2.7(b)(5), periodic evaluation of compliance with cyber security standards will be performed by an independent auditor.

To ensure cyber security, the following measures will be implemented in accordance with best practices and applicable standards:

Network Security

The Facility's computer network will be secured from malicious attacks to the greatest extent feasible. The network perimeter will be protected with defense technology, such as firewalls. A record of known unauthorized access attempts will be upkept. When a threat to network security is resolved, the Facility's response will be reviewed to evaluate potentials for improvement. Periodic audits will be completed to validate and evaluate current network security measures.

Malware Prevention

Malware is computer software that is maliciously installed to compromise cyber technology, including computers, networks, and servers, and other devices. The Facility will implement numerous technology solutions to combat the threat of malware, such as firewalls and anti-virus software. These measures will avoid, detect, and combat the threat of malware. Additional cyber security policies will be developed, as applicable and appropriate, to decrease vulnerability to malware.

Removable Media Controls

Removeable media, such as memory cards and USB flash drives, poses a threat to Facility security, as it can potentially be used to install malware or download confidential Facility information. Policies will be implemented to control the safe and responsible usage of removeable media. Facility cyber infrastructure will be stored in restricted-access areas and monitored by video surveillance and motion-activated lighting. Cyber infrastructure will be password protected, with limited personnel authorized to access sensitive infrastructure. All computers will reject removable media unless otherwise authorized.

Secure Configurations

All cyber infrastructure will be configured to be safe, secure, and efficient. A known secure configuration will be maintained from a baseline for the system. When required, software updates and patches will be installed to upkeep security and efficiency. All updates and patches will be reviewed and tested locally prior to installation to avoid unintended secondary impacts. Whenever possible, updates will be performed during periods of low activity to avoid adverse impacts to systems or inconveniences to personnel. Only authorized personnel will have software installation privileges. Devices, networks, and software will be periodically inventoried. Critical security threats will be reviewed and remedied as soon as possible.

User Education and Awareness

All Facility personnel with access to the Facility's cyber infrastructure and computer network will undergo cyber security training. All personnel working near the Facility control systems will be trained on cyber security policies and best practices. Personnel will be trained to assist in the detection of unauthorized cyber access attempts. Additional cyber security trainings and events will be completed at regular intervals.

Management of User Privileges

Only authorized personnel will have access to Facility cyber infrastructure. All authorized personnel will be provided with accounts with privileges restricted as appropriate to their role at the Facility. A limited number of authorized personnel will be provided with expanded access and privileges to critical infrastructure. These expanded accounts will be allocated on a strictly need-only basis. Contractors and consultants may be provided user accounts only when necessary; contractors and consultants will be required to follow all Facility cyber security policies. All authorized technology users must use secure passwords and update their passwords regularly. Users will be warned that accounts and services, such as email access, are subject to monitoring

by Facility management. Rights to accessing cyber infrastructure will be routinely reviewed and modified by the Facility Manager or Information Technology Director. In the event that personnel cease employment at the Facility, their accounts and user access will be terminated as soon as possible.

Incident Management

The Facility and O&M Service Provider(s) will establish procedures for responding to cyber security threats and violations. If cyber infrastructure becomes compromised, vulnerable, or non-essential equipment will be shut down as appropriate to prevent propagation of an attack. All incidents of malicious attack will be reported to the relevant authorities.

Additionally, the Facility and O&M Service Provider(s) will establish procedures for preparing for and responding to high impact incidents, such as fire, flood, and extreme weather events. During these incidents, critical records and data will be protected and recovered to the greatest extent feasible.

Cyber security exercises will be conducted periodically to test and audit Facility response to a cyberattack or natural disaster.

Monitoring

Cyber technology usage, including network traffic, will be monitored. Usage reports will be produced periodically to assess the efficiency and security of the Facility network and cyber infrastructure. If unusual activity is detected, it will be treated as a potential cyber threat and will be addressed accordingly.

6(e) Training and Recordkeeping

All Facility personnel, contractors, consultants, and visitors shall complete site security orientation and training upon first entry to the site and as needed. Records of Facility visitation will be documented. Known security threats and violations will be documented and recorded.

The SSP will be reviewed and updated as needed to address evolving security needs.

Appendix A:
Facility Overview for Emergency Response

Appendix B:

Local Public Safety Agencies and Emergency Service Providers

Local Public Safety Agencies and Emergency Service Providers

In the event of emergency, dial 911

Ames Volunteer Fire Department
Chief Shawn Bowerman
595 Latimer Hill Road, Ames, NY 13317
(518) 673-3044

Canajoharie Police Department
Chief Raymond Renzi
75 Erie Boulevard, Canajoharie, NY 13317
(518) 673-3111

Canajoharie Volunteer Fire Department
Chief Frank Nestle
75 Erie Boulevard, P.O. Box 28, Canajoharie, NY 13317
(518) 673-3812

Charleston Fire Department
Chief Randy Hulbert
1412 East Lykers Road, Sprakers, NY 12166
518-922-6706

Lake Valley EMS
Director of Operations Thomas Pasquarelli
P.O. Box 11, Amsterdam, NY 12010
Admin: (518) 843-1150
Dispatch: (518) 842-1777

Montgomery County Sheriff's Office

Sheriff Jeffery T. Smith

200 Clark Drive, P.O. Box 432, Fultonville, NY 12072

(518) 853-5500; (518) 673-2554; (518) 736-1850

Montgomery County Emergency Management Office

Director Jeffrey R Kaczor

200 Clark Drive, P.O. Box 338, Fultonville, NY 12072

(518) 853-4011

After Hours Emergency: (518) 853-5500

New York State Police

Troop G, Zone 3

Cobleskill Station – 950 Mineral Springs Rd., Cobleskill, NY 12043

Fonda Station – 3003 State Highway 5S, Fultonville, NY 12072-9703

(518) 630-1700

Rural Grove Volunteer Fire Department

Chief Kyle Kamp

1192 NY-162, Sprakers, NY 12166

ruralgrovevfd@yahoo.com