CFIUS Mitigation in Renewable Energy
Lessons Learned

Renewable energy transactions can raise potential threats to critical infrastructure as well as proximity issues of concern to the Committee on Foreign Investment in the United States (CFIUS). CFIUS Monitoring Agencies (CMAs) have recently signaled increased attention to the industry.

Kaerus Consulting LLC (Kaerus) was involved in execution of one of the first National Security Agreements (NSA) in the solar industry. We participated in the development and implementation of auditable controls to address, at the time, broadly-defined and nonspecific security risks. We then worked with CMAs to refine monitoring requirements for risks specific to the industry that became apparent. This article shares our experience.

Renewable Energy Economics

Renewable energy site development is expensive in money, time, and land. Not all locations are suitable for production as well as for meeting the requirements for a profitable power purchase agreement with a local or regional utility. Due diligence on projects in the United States takes two to three years and another two for construction. Sites are constructed with an approximately twenty-five-year expected lifespan, with the expected decommissioning cost priced into the financing.

In the past, site developers were separate from both owners and operators. Owners would purchase the sites from developers when a power purchase agreement was signed with a utility company. In the past two years, smaller developers have begun to build and operate sites on their own with no definitive plans to sell. As wholesale power rates increase, offers to purchase renewable energy sites, including by foreign investors, will rise.

Non-owner operators can be problematic for mitigation of national security risks. They are often not parties to NSAs and have no incentive to incur the costs of mitigation mandated by CMAs. Making them NSA signatories constrains owners should they want to change operators at a later time. One possible solution is for owners to contractually oblige operators to support the owner's NSA requirements and CMA mandates when they are hired, in the same way that large government contractors oblige their subcontractors to follow "flow down" requirements. Operators are likely to seek compensation for the costs associated with compliance.

Industry Regulation

Power production is highly regulated and monitored. Most facilities of interest to foreign investors will big enough that they will be required to comply with the North American Energy Regulatory Corporation (NERC) standards. These standards govern almost all aspects of bulk power generation and transmission in the United States, and are the widest-adopted energy standards in the industry. Since they are so well understood by the industry, the NERC framework should be used to measure and document compliance, even if a particular site is not large enough for the NERC standards to be required.

Site Security

Renewable energy sites are not designed and built to be "secure." Theft, of easily-transportable materials such as copper cable, scrap metals, and tools, is common. Owners and operators regard theft as a cost of doing business because losses are typically much less than the cost of prevention. For example, the cost of guard service at one site was approximately four times the cost of historic losses from theft, and did little to deter criminals in any case. Owners and operators may therefore demonstrate more resistance to adopting security measures than managers in other industries overseen by CFIUS.

Fortunately, there is little demand for scrap from potentially sensitive equipment, such as used combiner boxes and transformers. The devices that move power from the field to the transformer yards are immobile and provide little to no incentive for tampering or theft. Of the sixteen break-ins suffered by one owner of three facilities over a four-year period, ten were in storage areas for tools and cabling, three were in the transformer yards, and three were in solar arrays. In the solar arrays, only one resulted in theft. This is typical of what we see at other facilities and hear from the operator and maintenance (O&M) personnel in the industry.

Substation Control Centers (SCCs) are one of the most sensitive areas at sites for National Security concerns, but they are rarely targeted and have relatively strong security. Any attempt to compromise a facility as a whole would require undetected physical access to the SCC. Thefts close to SCCs typically consist of cutting copper grounding wire from the power line trenches to adjacent transformers. Such thefts carry a high risk for personal injury, but they are fortunately rare, have no impact on national security, and have a minimal impact on site operations. Most SCCs have steel construction, robust locking mechanisms, and access control systems. These ease the process of inspection and enable control over physical access to critical components.

Physical Security Measures

Perimeter chain link fencing with barbed wire is the most common physical security measure employed at renewable energy sites; however, it is intended to deter accidental access to potentially dangerous areas rather than to prevent an attacker from accessing a site. Further, environmental agencies often impose restrictions on fencing, to allow the passage of wildlife for example, which create weaknesses that can be exploited by an attacker. Water, wind, and erosion also take a toll on the effectiveness of physical barriers. In short, fencing is unlikely to deter attackers.

Closed circuit television (CCTV) systems are not required by energy regulatory agencies. In some cases, insurance carriers provide incentives to install them, but many facilities are built without CCTV systems. When installed, CCTV systems are designed to meet the bare minimum requirements to qualify for insurance premium incentives. Further, they are rarely tested and minimally maintained. They are therefore unlikely to meet CMA expectations.

Other deterrents, such as guard patrols and perimeter and interior lighting, have not proven successful in our experience. Even common thieves can observe and avoid patrol patterns. Such measures can, however, help to *detect* unauthorized access.

In a recent case, overt guards, whose deterrent value had been determined to be minimal, were withdrawn from a site and replaced by low-profile static surveillants. A possible thief was detected casing the site, returning to cut a lock, and then returning once again to presumably enter the site to steal materials. The individual departed rapidly when a surveillant approached him. This episode illustrates that thieves targeting renewable energy sites case their targets, note deterrents, avoid them, and avoid contact with site personnel.

Physical security measures are unlikely to prevent access to most areas of sites. Detection after the fact is a more realistic expectation.

Impact of Unauthorized Physical Access

The installation or modification of equipment for persistent data collection is likely to leave observable evidence. Further, the physical modification of site devices is nearly impossible to complete without triggering an alert from the site's Supervisory Control and Data Acquisition (SCADA) system. In short, the physical modification of the array or installation of collection equipment is a possible risk but manageable through a robust periodic inspection and documentation process.

Network and Data Security

The SCADA system is the core of a power-producing facility's network. SCADA systems monitor and control the flow of information from a production facility to the local or regional grid to which it connects. The system controls equipment, transfers data, and measures power transferred. It further allows for both remote and local control of the power facility, allowing for production curtailment, disconnect, shutdown, etc. The system is subject to maintenance, monitoring, and inspection by the utility company. Because the SCADA system is used to calculate payments owed by the utility, it is typically very well maintained.

Renewable energy sites have additional information security (IS) systems. In some cases, the O&M company has its own internal IS staff, and in others, IS is outsourced. The objectives of IS are to maintain the security of the network and its equipment, manage and monitor access, mitigate identified vulnerabilities, and thwart and report on attacks, outages, and other IS and SCADA-related concerns. IS staff also monitor the CCTV system, which constitutes a vector for system access. For NERC-compliant sites, we have seen no overlap between the CCTV, SCADA, and other IS systems. However, in smaller sites, we have seen devices and equipment with access to both the SCADA and CCTV systems. The best practice is to segregate all other CCTV and IS systems physically and logically from the SCADA network.

Procurement

Only a handful of Original Equipment Manufacturers (OEMs) produce renewable energy equipment. Equipment selection is most often dictated by the local or regional utility to which the power is sold. Changes to OEM Equipment (for the most part) are unusual because components are not necessarily designed to be interchangeable. Fortunately, component failure is rare and typically handled by the OEM.

The identification and regular inventory of sensitive equipment is the only means of detecting potential procurement risks. Federal contract regulations, such as the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), provide supply-chain security standards. Where possible, both U.S. and foreign-made equipment should be sourced directly from the manufacturer.

Reporting

While demonstrating compliance in any security endeavor is challenging, it can be particularly difficult in renewable energy because of the number of players. Working with company management, O&M contractors, regulators, local law enforcement, CMAs and other CFIUS-mandated monitors can require flexibility, negotiation, and patience. Stakeholders must agree on reporting thresholds, monitoring criteria, and a reporting cadence that meets the CMAs' needs. Discussions should focus on what actually impacts National Security and how can it be measured.

Existing IS tools are invaluable to monitor compliance with agreed-to requirements regarding network and data security. Most reporting tools can provide:

- Changes to authorized access.
- Descriptions of software and hardware changes.
- Patched and unpatched vulnerabilities.
- The number of thwarted access attempts.

Typically, standard IS reporting tools can be effectively combined to meet agreed-to requirements. We have yet to come across a facility where this is not the case.

Physical access is also straightforward to document. This process is only confounded by the volume of outsourced maintenance activity, which accounts for less than 20% of the maintenance required onsite, but accounts for more than 90% of the site access concerns. Specialized maintenance, such as for high voltage transformers, is relatively rare and is conducted by highly trained technicians if not by the OEM technicians themselves. General maintenance such as weeding, road maintenance, fence repair, etc., is typically outsourced to local vendors which can create access control issues, especially when they have foreign citizen employees.

Due to the number of sub-contractors who require access to renewable energy sites, badging systems have proven to be insufficient for documenting access. There are however many

supplementary access-control tracking systems available on the market. The use of a single system that can account for both employees and subcontractors is certainly preferred.

CCTV metrics are challenging and must be developed from scratch in most cases. We utilize a system of monitoring individual camera uptimes, alarms generated, sent, received and those adequately processed. In each case, this has required extensive training of both the O&M and the CCTV monitoring company's staff. Large providers are unlikely to be flexible enough to provide customized reporting, and we have found that mid-sized providers tend to provide superior responsiveness. Finally, both CCTV monitoring and CCTV maintenance should be conducted by the same company. Otherwise, separate companies will likely blame the other for any problems. With a single point of failure, there are fewer failures.

Contact: Albert Schultz, 571-243-2492, albert@kaerusllc.com