BURNS McDONNELL

CASE STUDY / **SUBSTATION SECURITY PROGRAM**

PREPARING CRITICAL SITES AGAINST DIVERSE THREATS

Physical security at substations — against natural and malign threats — has become an increased focus for utilities. One Midwestern utility took steps to get ahead of the regulatory curve, seeking to develop and implement an aggressive, comprehensive strategy to harden its critical substations.

REACTION TO REGULATIONS FUELS COMPREHENSIVE ASSESSMENT

An adaptable approach provided a framework to prepare different sites for a range of potential challenges.

PROJECT STATS

CLIENT
Confidential

LOCATION
Midwestern U.S.

DURATION
Two years

2
STATES

6
THREAT METRICS EVALUATED

15
SITES ASSESSED

CHALLENGE

In 2014, the North American Electric Reliability Corp. (NERC) issued a set of critical infrastructure protection requirements known as CIP-014, intended to establish effective physical security standards at the sites where the nation's grid was most vulnerable. These requirements made it necessary for electric utilities to evaluate their assets and prepare a response.

One Midwestern utility with assets spanning two states moved swiftly to begin exploring appropriate measures under the CIP-014 process. It initiated a pilot program to examine threat vectors and evaluate existing security plans, both physical (barriers, lighting and technology) and programmatic (strategy, staffing and incident response protocols).

The utility's early efforts with a consultant were not satisfactory; management felt it was being pushed to accept options from a set of cookie-cutter solutions. The utility opted to engage Burns & McDonnell to develop a more customized approach and address any deficiencies from its prior efforts.

SOLUTION

We recognized the client's priorities were to develop a security strategy congruent with its unique threat landscape and site vulnerabilities, as well as to more effectively leverage its security budget. The objective of the pilot program was to deter and detect any acts of terrorism, attempted breaching of the site, and potential harm to critical equipment in each substation.

After conducting a thorough assessment, 15 priority sites were identified, representing a mix of urban and rural locations. For these sites, the client needed answers to some key questions:

- Which technologies are most appropriate for each site?
- What is the right solution — or combination of options — for walls and fences?
- What impact will security elements have on the safety of the substation and its transmission interconnection?

After visiting each site and assessing them on six threat metrics — ranging

from theft or an active shooter to improvised explosive devices — our team provided solid answers, measurable outcomes and mitigation recommendations. Our visits also included performing OPFOR (Opposing Force) activities to test the security devices in place, both physical and technical. We worked closely with utility operational and security staffers to develop a solution set that integrated seamlessly into their system.

We prepared reports on recommended security measures for each critical site, formatted to meet the requirements of the CIP-014 standards. We also prepared detailed designs, including tailored upgrades at several substations. These employed concrete T-walls of various heights and anti-cut/anti-climb fencing, as well as electronic surveillance upgrades.

Our professionals reviewed survey data and existing station drawings to evaluate clearances, develop modified site plans, determine fence heights, and define design and fabrication details for barrier manufacturers. We also provided construction management support as the utility implemented some of the recommendations, extending our project assistance from beginning to end.

RESULTS

The pilot program successfully enabled the client to meet its then-imminent CIP-014 requirements and better position itself for future regulatory changes. The work was completed on schedule and within budget.

For the utility, the primary benefit of the program was the development of an adaptable, replicable approach that could adjust from basic to complex threat environments, whether natural or malign. The utility could escalate or de-escalate as the threat landscape changed. The methodology could be easily demonstrated to auditors and provided a valuable framework for reviewing and addressing a variety of potential challenges.

BURNS McDONNELL

burnsmcd.com | Offices Worldwide

18344-SSP-0920