Enforcement Explained

Public

By: Mike Hattery, Counsel

Physical Security Common Failure Points

Physical security is a constant concern at ReliabilityFirst and the ERO at large, but it has been thrust to the forefront of national discussion of late following attacks on multiple substations. Here we'll explore some common failure points that we are seeing in the physical security space in terms of both preventive controls and breach identification controls.

Taking a proactive approach to preventative controls is essential

The central requirements for entity physical security plans and protections for Physical Security Perimeters (PSPs) rest in CIP-006-6, and elevated requirements around certain transmission stations, substations and primary control centers rest in CIP-014-3. Additionally, requirements for low-impact sites rest in CIP-003-8.

Specifically, when it comes to CIP-006-6 R1.1-R1.3, one of the most common issues we see is Physical Access Controls Systems (PACS) failing, and as a result, adversely impacting PSP security. We've seen this come up during a transition to backup power (i.e., loss of primary power supply) or after a PACS restart (e.g., can occur due to power disruption, during transition to backup power, or following maintenance). In these scenarios, the PACS failure typically results from delayed or fragmented restarts.

It is important for a registered entity to understand how access points will function in these scenarios (e.g., fail safe versus fail secure). Another issue in device restarts that can arise is, when restored, sometimes the settings can revert to prior versions creating incompatibility or a lack of correct access lists.

This is where CIP-006-6 R3.1 maintenance and testing function as such an important control. Testing PACS at least every two years is essential, and a proactive entity will test PACS with more frequency and in varying scenarios (i.e., after a cold restart or some other disruptive event). Another useful tool is utilizing security walkdowns of facilities to test different PACS devices and access controls to assure functionality.

An effective walkdown might include testing PSP doors to ensure they are closed and secured, prompting alarms to see if they function as intended and reviewing camera angles to assure they are capturing appropriate areas. Adding surface-level PACS testing to physical security walkdown checklists is a solid step in improving the probability that a non-functional PACS will be identified and remediated quickly.

Continued on page 14

Enforcement Explained

Continued from page 13

When it comes to CIP-014-3, we’ve identified some shortcomings in R1 risk assessments through our compliance monitoring and enforcement activities (e.g., scope of facilities and contingencies studied).

These shortcomings can create issues when it comes to identifying and protecting critical facilities, so we encourage registered entities to proactively evaluate their approach to R1 risk assessments and reach out to our Entity Engagement team if they have questions regarding their approach to CIP-014-3 analysis, as opposed to waiting for a compliance monitoring engagement. And, as far as reducing the overall risk to the Bulk Electric System, it is worth highlighting that ReliabilityFirst has observed some registered entities adopt a best practice approach of implementing heightened physical security protections at more facilities.

Contact Entity Engagement

We encourage registered entities to proactively evaluate their approach to R1 risk assessments and reach out to our Entity Engagement team if they have questions regarding their approach to CIP-014-3 analysis.

Do not fall victim to alarm apathy

Increasingly, being nimble in terms of limiting damage and executing expedited restoration requires near instantaneous response to alarms indicating a potential breach attempt. One of the root causes or fact patterns of concern for ReliabilityFirst relates to alarm apathy. For several entities in the ReliabilityFirst footprint, central security will encounter a number of false positive alarms for PSPs on a daily basis (including remote locations where deployment may be necessary).

This is a physical security struggle that Aesop’s “The Boy Who Cried Wolf” foretold, constant alarms and notifications leading to an atrophy of attention for when the actual wolf (attempted breach) appears.

One of the points well-articulated in February’s Technical Talk with ReliabilityFirst was that without proactivity in response to alarms, their existence becomes moot. With this in mind, we encourage entities to emphasize the importance of timely investigating all alarms to their security groups and staff at large. Additionally, consider evaluating recent alarm response times, and assess whether more aggressive action needs to be taken. Finally, entities should review their central alarm interface to determine if changes need to be made to alarms or notifications to reduce unnecessary noise.

Vigilance is key

In terms of the failure points discussed above, there is one cultural theme that is essential, vigilance. Entities have to support a culture of vigilance among both their security and non-security staff. Be it performing proactive walkdowns to assure functioning PACS, increased scenario testing for PACS devices, or behaving as if each alarm could be the real thing, doing these things effectively requires a culture of vigilance.