NATF Practices Document for NERC Reliability Standard CIP-014-1 Requirement R5

Disclaimer

Open Distribution

Contents

References

NERC Reliability Standard CIP-014-1

NERC Glossary of Terms

Revisions

Date	Version	Notes
June 25, 2015	1.0	Original Version

Section 1 Purpose

The purpose of this document is to provide a NERC Reliability Standard CIP-014-1 Requirement R5 Practices Guide containing an approach, common practices, and understanding for the development and implementation of Physical Security Plans.

Problem Statement

NERC CIP-014-1: Requirement R5 states:

Each Transmission Owner that identified a Transmission station, Transmission substation, or primary Control Center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary Control Center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*
- *Law enforcement contact and coordination information.*
- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*
- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary Control Center(s).*

Scope

The scope of this project was to develop a NERC Reliability Standard CIP-014-1 R5 Practices Guide containing approaches and descriptions of common terminology and understandings that are defensible (but not prescriptive) for developing and implementing Physical Security Plans as specified in Requirement 5. The intent is to assist and facilitate NATF Members when developing and implementing Physical Security Plans to satisfy this Requirement R5.

Section 2 Definitions

Glossary of NERC-Defined Terminology

Electric Reliability Organization (ERO) – NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.

North American Electric Reliability Corporation (NERC) – A not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people.

Physical Access Control System (PACS) – Any asset that controls, alerts, or logs access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Team-Recommended Terminology

Access Control System (ACS) – A means of electronic access where the access rights of personnel are predefined in a computer database. Access rights may differ from one physical perimeter to another based on some defined, needs-based criteria.

ASIS – ASIS International is an organization of security professionals. ASIS membership develops security standards, expertise based certifications, and offers training in the area of physical security.

Ballistic Shielding – A physical security feature with the purpose of protecting or minimizing damage from an attack on an asset.

Closed Circuit Television System (CCTV) – A camera system in which signals are not publicly distributed, but are monitored primarily for surveillance and security purposes. CCTV surveillance can be very effective in operational settings. Record analog or digital video surveillance that captures and stores images of activity in the site/facility preceding a site/facility security alarm can provide the system operator a "quick review" of the site/facility alarm incident and assist in the subsequent incident investigation.

CPP (see also PSP) **–** The Certified Protection Professional, an ASIS International (ASIS) certification, demonstrates knowledge and experience in eight broad Security areas including: Principles and Practices, Business Principles and Practices, Investigation, Personnel Security, Physical Security, Information Security, Crisis Management, and Legal Aspects.

Crime Prevention Through Environmental Design (CPTED) – Crime prevention through environmental design is an approach to problem mitigation that considers environmental conditions and the opportunities they may offer for crime prevention or the prevention of other unintended and undesirable behaviors. CPTED attempts to reduce or eliminate those opportunities by using elements of the environment, either natural or man-made, to control access, provide opportunities to see and be seen, define ownership, and encourage the maintenance of property.

Defense in Depth/Layered Security – A strategy that seeks to delay rather than prevent the advance of an attacker to an intended target, allowing time for detection and response. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on multiple layers of defense allowing time for detection and analysis of the threat and, if necessary, response to the incident.

Electric Sector Information Sharing and Analysis Center (ES-ISAC) – NERC department providing a trusted capability for sharing sector Electric Sector specific information by collecting, analyzing, and disseminating alerts and incident reports; working with government agencies to ensure sector specific technical details are accurately understood; coordinating with other sector ISACs and international groups; and providing for mutual information sharing during disruptions.

Emergency Power – Consideration should be given to the power supply and all security equipment, such that a temporary outage or throw-over of source will not create a recycle period on the electronics, which creates a dead period.

Fencing – This is the minimal physical security asset and usually defines the first physical security perimeter encountered at a site/facility. There are several levels of fencing ranging from solid material, standard chain link fencing (most common), cable-reinforced chain link fence, and anti-cut, anti-climb grade fencing. This will normally be one of the first layers of defense against a potential intruder at the perimeter to a site/facility.

First Responder – The first to arrive at and assist at the scene of an emergency, with a duty to act. This would typically include police, firefighters, and emergency medical responders such as paramedics and emergency medical technicians. They may also include private security and facility personnel.

Fusion Centers – A state or regional government organization that focuses on information sharing and all-hazards intelligence to prevent acts of terrorism. Fusion Centers are generally a multidiscipline, multi-agency network of professionals, which may be comprised from any of the following entities: private sector, local, state, tribal, and Federal partners. The purpose of a Fusion Center is to prevent, protect and respond to crimes and potential or actual acts of terrorism. Fusion Centers are centralized resources that gather, analyze and share information by disseminating it back out to respective entities. Each Fusion Center is a component of the national network of Fusion Centers, which are an integral part of the U.S. Department of Homeland Security's strategic initiative for information sharing.

Intelligence – Information or analysis of information that defines a potential threat. This information typically comes from Suspicious Incident Reports (SIR), Suspicious Activity Report (SAR), law enforcement, state and Federal authorities, or other organized entities that may gather, analyze and disseminate such information.

Intrusion Detectors – These devices use various means such as motion, sound, infrared, or optical beam to detect intrusion through or in a specific area.

Law Enforcement – A Federal, state or local agency or entity comprised of trained, sworn/commissioned, policing professionals, with the responsibility of enforcing and upholding the laws of a jurisdiction.

Lumen – A unit of measurement for the brightness of light within a given space. Guidelines for recommended levels are published by various groups, including the industry's Illuminating Engineering Society (IES).

Physical Attack – An attack, of a physical nature, that can result in injury to personnel and/or destruction of property, reduced operability, and loss of personnel or facility capability.

Physical Perimeter – A border surrounding a given space, building(s), or room(s). A perimeter may be comprised of walls, fencing, or detection systems, alone or in combination that restrict or exclude access, promote detection, and indicate ownership.

Physical Security – Security measures designed to deter threats or mitigate vulnerabilities such as fencing, lighting, guards, access control hardware, signs, and environmental features.

PSP (see also CPP) **–** The Physical Security Professional, an ASIS International (ASIS) certification, provides demonstrated knowledge and experience in threat assessment and risk analysis; integrated physical security systems; and the appropriate identification, implementation, and ongoing evaluation of security measures.

Physical Security Plan – A plan outlining physical security measures, notification protocols for incidents and response measures to potential threats and actual incidents with defined roles and responsibilities. A Physical Security Plan may incorporate mitigations for vulnerabilities identified and defined in a physical security assessment.

Physical Security Perimeter **–** The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

Reliability Coordinator – The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.

Security Feature – An aspect of a physical security component, technology, or mitigation measure.

Security Measures – Actions, policies, or procedures designed to deter or mitigate specific security risks and vulnerabilities.

Security Operations Center (SOC) **–** A centralized organization or unit that deals with physical and/or cyber security issues, at an organizational and technical level. A Security Operations Center within a building or facility is a central location from where staff may monitor and supervise local or remote site security, using data processing and security technology. Typically, it is equipped for electronic access and CCTV camera monitoring, and controlling any number of access control, security, and related communications systems.

Security Risk Assessment – A physical security oriented objective analysis and review, utilizing pre-determined criteria, of the current security controls resulting in an assessment that defines vulnerabilities, categorizes potential threats, and produces a risk score that allows for comparison and prioritization for the prevention of the loss of assets. From this assessment, it can be concluded how critical each asset is and which assets require protection.

Threat – The intent to conduct harm or capitalize on an actual or perceived vulnerability that could result in damage, destruction, or loss of life or property.

Transmission Operator – The entity responsible for the reliability of its "local" transmission system and that operates or directs the operations of the transmission facilities.

Transmission Owner – The entity that owns and maintains transmission facilities.

Transmission Station/Substation – An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.

Video Analytics – A technology that enhances video surveillance systems by performing the tasks of real-time event detection, post-event analysis and extraction of statistical data while saving manpower costs and increasing the effectiveness of the surveillance system operation. By defining the set of events that the surveillance system operator wants to be alerted to, the video analytics software continuously analyzes the video in real-time and provides an alert upon detection of a relevant or pre-defined event.

Vulnerability – A weakness or a gap that potentially may be exploited by a threat.

Vulnerability Assessment – Within the context of CIP-014, a systematic evaluation process of a Transmission station(s), Transmission substation(s), and primary control center(s) to identify, quantify and prioritize the vulnerabilities or weaknesses of the location and its assets. The goal of a Vulnerability Assessment is to identify weaknesses to which mitigations may be applied.

Wall – An upright structure, either freestanding, extension or part of a building that, provides a physically impenetrable barrier from one area to another. A wall may be constructed of different materials such as brick, concrete, wood, or metal.

Section 3 Guide

Requirement R5

Requirement R5 – Each Transmission Owner that identified a Transmission station, Transmission substation, or primary Control Center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary Control Center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

Using the results from Requirement R4 (Threat & Vulnerability Assessment) identified threats and vulnerabilities must be addressed by specific mitigation strategies in the physical security plan. These mitigation strategies will be used to protect against or minimize the impact of physical attacks.

Because of the unique nature of each facility, it is recommended that a site-specific security plan be developed for each Transmission station, Transmission substation and primary control center identified in Requirements R1 and/or R2. To aid in this process, a sample physical security plan template is provided in Section 4 of this document.

Physical security plans are required to be developed within 120 days following the completion of Requirement R2. Although not required by the Standard, generally accepted security practices recommend that security plans be reviewed annually by an organization's senior management.

Requirement R5.1

Requirement 5.1 – *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

According to the NERC CIP-014 Guidelines and Technical Basis document, resiliency may include, among other things:

- System topology changes
- Spare equipment
- Construction of a new Transmission station or Transmission substation to distribute the load to several facilities versus concentrating in one

When deploying security measures for Transmission stations and Transmission substations, it should be decided whether to harden the entire facility or specific critical assets and infrastructure within the facility. This may not be possible for Control Centers.

While most security measures will work together to collectively harden the entire site, some may be designed to only protect specific critical components. For example, if protection from gunfire is used, the entity might only install ballistic protection for critical components and not the entire site.

A critical consideration in developing a comprehensive and adequate security plan is to determine the response time to a physical attack. Response could come from trained personnel, a dedicated security force, or local law enforcement. The response time will

determine the defense-in-depth and delay measures needed to protect the facility adequately. If the response resource is five minutes away, the number and/or coverage of security measures deployed may be minimal. Conversely, if the response resource is 30 minutes away, additional measures may be necessary.

To demonstrate the installation of the security measures specified in the physical security plan for a specific facility, it may be best to document them on a facility site map included as an attachment or appendix to the physical security plan or the facility.

Generally accepted security measures for a Transmission station, Transmission substation, and/or a primary control center used to mitigate documented threats and vulnerabilities include:

Deterrence Measures

Visible physical security measures installed to persuade individuals to seek other, less-secure targets.

Examples:

Perimeter signage – Placed on the entire perimeter and at entrance points to declare "No Trespassing" and that the facility is actively monitored, or similar messaging. Placement of signage should be so that all signage is clearly visible and legible from any location along the entire perimeter.

Environmental Design – Entities should consider using the principles of Crime Prevention Through Environmental Design (CPTED, see www.cpted.net). CPTED promotes the principles that proper design and effective use of the environment can lead to a reduction in the incidence of crime and acts of terrorism.

Fencing / walls / gates / natural barriers – The most basic outer layer of protection to deny and delay access to a facility. All barriers of this nature are rated in method of construction, material, and time of delay (from a few seconds to minutes or hours). When installing perimeter barriers around critical sites, consideration should be given to:

- Constructing the barrier to prevent scaling
- Incorporating vehicle, bullet, and blast protection or deflection
- Limiting visibility, where appropriate, inside the facility and protect from the threats identified in Requirement R4.
- Installing gates with the same level of protection as the fence / wall / cables
- Installing two or more fence lines to build in delay time, creating a "dead zone" for monitoring where no motion would be anticipated, and installing vehicle traps to prevent tailgating authorized vehicles
- The hardware used for installation of these components such that the component cannot easily be disassembled/neutralized (example – most chain link fence is installed with soft aluminum wire ties; consider hardened ties or carriage bolts secured from inside instead with additional precautions to anchor and tension the lower edge).
- Not using automatic exit beams or ground sensors on gates that could be used by perpetrators to provide access to other perpetrators or quick exit by initiating the sensor

On-site or Roving Security Officers/Other Trained Personnel – Armed or unarmed contracted or proprietary uniformed security officers or other trained personnel either

permanently located at a site or conducting frequent, periodic, and irregular vehicular or foot patrols.

Lighting – Security lighting enables personnel to maintain visual assessment capability, during the hours of darkness. When developing a lighting plan for a critical facility, consideration should be given to:

- Maintaining unlit interior station equipment with entry/motion/alarm-controlled yard lighting for transmission stations/substations to prevent external surveillance and potential target acquisition (creating a site through light deterrence)
- Maintaining lighting illumination levels at border and/or buffer zones integrated with surveillance systems to support the camera illumination specifications
- Collateral impacts (e.g., adjacent property, zoning restrictions) of the lighting systems deployed
- Strobe or flashing lights in conjunction with the detection systems to communicate to any intruder that they have been detected
- Lighting that provides minimum maintained illumination levels for pedestrian pathways, bicycle and vehicle routes, parking structures, parking lots, way finding, signage, pedestrian entrances, and building services in urban areas

Locks – Consider the use of a high-security locking system. This could include a controlled key (assigned, logged, and monitored) with a high-security lock that meets High Security Standards (such as Grade F5/S6 per the ASTM F883) and that has high security chains (>Grade 100 or high security square link design). In addition, an entity could consider puck locks with high-security hasps on all entries and critical equipment access.

Voice Down Capability – Consideration should be given to having installed voice down capability such that when an alarm is generated the Security Operations Center can speak to the intruder.

Detection Measures

Physical security measures installed to detect unauthorized intrusion and provide local and/or remote intruder annunciation.

Examples

Neighborhood Awareness Program / Neighborhood Watch – Awareness program created to educate and encourage citizens to vigilantly watch around their community or property and report suspicious behaviors or activity that may have connections to crime, including security threats to electric company facilities.

Security Operations Center monitoring – A central location from where staff manages or monitors access control systems, video surveillance, and possibly controls lighting, alarms, and vehicle barriers for remote site(s) using telecommunications, security and data processing technology. With the aid of technology, the electronic systems within the Security Operations Center or at the site detect suspicious activities allowing the Security Operations Center staff to assess the activity and initiate the appropriate response.

Sound Detection – Technology deployed to detect the sounds of movement and or gunshots/explosives and notify the Security Operations Center.

Intrusion Detection Systems – Physical intrusion detection is the act of identifying advancing or intruding threats. Physical intrusion detection is typically accomplished by physical controls put in place to detect entry into a defined security perimeter. Examples of physical intrusion detections may be security guards, access control systems, mantraps, vehicle traps, motion/vibration sensors, video surveillance, and other motion-detection devices.

Delay Measures

Physical security measures installed to delay an intruder's access to a physical asset and provide time for incident assessment and response. Delay tactics can incorporate Crime Prevention Through Environmental Design methods – See above Deter

Examples

Vehicle Barriers – Energy-absorbing barriers, cable systems, technical excavations, or reshaping of existing drainage deployed around the perimeter may be useful to prevent the threat of vehicle-borne improvised explosive device (car/truck bomb).

For example:

- Landscaping **–** berms, gullies, boulders, trees, and other terrain
- Hardscaping **–** benches and planters
- Structural **–** walls, bollards, and cables

Critical Component Protection – Critical components within a substation may be individually protected to increase the delay time required to allow for response. This may include individual barriers, protective coverings/coatings, or raising the critical component.

Multiple Layers of Delay – This is the key concept of the protection-in-depth methodology: numerous barriers deployed to slow or block an intruder's path to the intended target.

Buffer Zone Protection – A buffer zone is generally an area that lies between two or more distinct borders. In physical security terms, it is the area adjacent to the primary fence surrounding a substation or control center used to detect and/or to delay intruders, many times using the local terrain to the best advantage and/or deploying CPTED principles.

On-site Security Officers/Other Trained Personnel – See above Deter.

Fencing/walls/gates – See above Deter.

Assessment Measures

The process of evaluating the legitimacy of an alarm and determining the procedural steps required to respond.

Examples

Video Surveillance – The use of cameras for video surveillance can be effective in operational settings. An example of pre-processed video surveillance would be the review of video history recorded prior to an alarm being generated, which allows Security Operations Center personnel to "see" what occurred prior to the alarm. This is invaluable valuable resource for Security Operations Center personnel during their alarm assessment and prior to initiating response.

Video Analytics – Video analytics is the technological capability to detect and determine events using the following aspects: temporal (meaning time intervals) and spatial

(meaning space and the relationship of objects within it). The temporal and spatial algorithms can be implemented as software on general-purpose machines or as hardware in specialized video processing units. Video Motion Detection is one of the more simple forms where motion is detected with regard to a fixed background scene and an alert is generated to those responsible for monitoring. More advanced functionalities include video tracking and egomotion estimation. (An example would be estimating a person's moving position relative to lines on the parking lot.) Because video analytics is generated in the device, it is possible to build in other functionalities such as identification, behavior analysis, or other forms of situation awareness.

Security Operations Center – See above in Detect.

Communicate

Communication systems used to send and receive alarm/video signals, audio, and data. Also, includes the documented process to communicate detected intrusions.

Examples

Security Operations Center Initiates Response – Documented and exercised procedures should be followed to initiate response on suspected or known incidents. All communications should be clear, concise, and thorough using plain language. Routine contact should be made, in accordance with established procedures, with the Transmission Operations Center to help Security Operations Center personnel determine if approved personnel are on site, if equipment alarms/events are occurring at this site or adjacent sites, or if adjacent communications paths have been interrupted. Information of this nature might heighten the level of concern regarding activity or alarms being generated at a Transmission station(s), Transmission substation(s) and primary control center(s).

Signal and Data Transmission – Data transmission, digital transmission, or digital communications is the physical transfer of data (a digital bit stream) over a point-to-point or point–to-multi-point communication channel. Examples of such channels are copper wires, optical fiber, wireless communication channels, storage media, and computer busses. The data is represented as an electromagnetic signal, such as an electrical voltage, radio wave, or infrared signal. Consideration should be given to protecting the communications path back to the Security Operations Center. An uninterrupted power supply should be considered for communications and security equipment to prevent blind periods during reboot or restart after a power interruption or throw-over operation.

Recording Methods – Many Security Operation Centers record and time stamp all two-way radio and telephone communications as well as surveillance system information. Recordings are especially useful for process improvements and to assist in investigations and event reconstructions.

Alarms and Display – Consideration should be given to the configuration of the Security Operations Center for maximum internal visibility of all alarm and security displays without clutter, which may include having CCTV and access system alarms displayed on separate, dedicated video monitors.

Intercom System – An intercom system is useful to receive communication from remote access points. In addition, it can be used to query unverified individuals attempting to access or where access has been rejected (see Voice Down in Deter section).

Respond

The immediate measures taken to assess, interrupt, and/or apprehend an intruder.

Examples

Documented Procedures – Each organization should have documented response procedures to train responders and to assign responsibilities. The procedures should be regularly tested and reviewed/revised on a recurring basis.

Responses to Alarms – Automatic responses exclude human intervention when an alarm is received. Manual responses normally involve some aspect of human process before a response is initiated.

State or local Law Enforcement deployment – This will normally be the armed responding force when a physical attack is underway. Coordination with and awareness by local law enforcement officials will be the key to rapid response. See more in Requirement 5.2 below. A predetermined response level should be provided for various levels of events.

Armed Security Officer Deployment – Subject to local laws and regulations, some organizations may have their own armed private response force for responding to a physical attack.

Most facilities identified as critical under this standard will also probably be deemed critical under the NERC cyber security standards. Many of the strategies deployed for CIP-014 will build upon and support the cyber security standard requirements.

Generally, accepted security practices recommend the periodic testing of deployed security systems.

Requirement R5.2

Requirement 5.2 – *Law enforcement contact and coordination information*.

A list of first responding local law enforcement, fire, emergency management and emergency medical services contact information should be included in each site-specific security plan. If military assistance may be available, their contact information should be considered as well, and any legal or governmental contacts or memoranda of understanding [MOUs] within the organization needed for their utilization such as the State Emergency Management Agency and their Joint Task Force group. Contact information may include agency name and contact name with telephone number(s) and email address, title, and address. An alternate contact for each should be considered in accordance with corporate policies.

A robust coordination and training program would include substation safety and familiarization for first-responder contacts and familiarization tours of primary control centers. Consideration should also be given to conducting joint emergency response exercises with your contact agencies as well. If areas around the sites are suitable for use as staging areas during a response, those may be given consideration and identified with the agencies. If there are specific training requirements (such as OSHA), research if they can be waived or if training could be abbreviated for first responders. Discuss communications protocols, escalation, and site access priorities vs. forensics. Ensure that BES Exceptional Circumstance procedures allow for their entry into any physical perimeter within the site during a response.

Site tours and training of local first responders / law enforcement is encouraged. Though not required for the standard, documentation of these meetings could be

recorded through agendas, dated presentations, meal receipts with lists of attendees, and site visitor logs.

Requirement R5.3

Requirement 5.3 – *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require the enhancements and modifications be completed within the 120-day security plan creation requirement. The actual timeline will probably extend beyond the 120 days, depending on the amount of work to be completed. Timelines should be reasonable, and recording multiple dates should be considered if security or resiliency measures are deployed in phases and/or on different dates. Timelines should be modified only with the approval of management, and the reasons for such modification documented and retained. If electrical resiliency measures are constructed to eliminate the site from applicability under Requirements 1 and 2, those dates should be reflected in the timeline as well, if they are known.

Requirement R5.4

Requirement 5.4 – *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary Control Center(s).*

An entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, Fusion Centers, and U.S. and/or Canadian Federal and state agencies. This information may be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in Requirement R5.

Some mechanisms and sources for current threat information could include the following:

- Telephone, email, or face-to-face meetings are beneficial to developing and maintaining partnerships for current threat information. Additionally, first responder alarm response may be discussed on a scheduled and/or recurring basis throughout the year.
- The ES-ISAC conducts a monthly series of hour-long webinar briefings at the ES-ISAC PRIVATE (Yellow) level of information sensitivity, covering critical infrastructure protection topics within and specific to the Electricity Sector. Representatives from the Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team and the Office of Intelligence and Analysis discuss current events that DHS is monitoring within the Electricity Sector. This call is reserved for electricity sector asset owners, operators, and their representatives and agents or where the ES-ISAC has made specific invitations to guests.
- The ES-ISAC produces a weekly email, *AOO Security Blog* that is sent to electricity sector asset owners, operators, and their designated representatives and agents.

- Most Fusion Centers support a Terrorism Liaison Officer (TLO) program. A TLO is an identified person within law enforcement, fire service, emergency management, health, military or the private sector that is responsible for coordinating terrorist and other criminal intelligence information from his or her local agency to the state or regional Fusion Center. The TLO program allows agencies throughout the state to combine resources and share information, thereby providing a clear picture for intelligence and threat analysis and allowing greater prevention, preparedness, and security efforts. The TLO is the direct point of contact for the state Fusion Center at the local level and is the key to the two-way flow of information from the TLO's region to the state Fusion Center.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews. A registered entity's physical security plan may include provisions for additional security measures or enhancements to existing measures, which could be deployed to address an evolving or imminent threat identified through the processes in Requirement R5.4. These measures could be implemented on a temporary basis during a period when there is a specific threat or vulnerability or on a permanent basis if the threat or vulnerability is assessed to be ongoing in nature.

Section 4 Physical Security Plan Template

A sample Physical Security Plan template begins on the next page. This is only a sample and may be modified to best suit each entity's particular needs to satisfy the requirements.

[Company Name & Logo]

Critical Infrastructure Protection

[FACILITY NAME]

Physical Security Plan
(NERC Standard CIP-014-1)

Version [#], [Date]

Table of Contents

Purpose

Detail the physical security plan and procedures to be implemented and executed by [COMPANY NAME] employees operating [COMPANY NAME] Critical Facilities. The plan incorporates North American Electric Reliability Council (NERC) and [COMPANY NAME] security requirements, guidelines, policies, and procedures.

Definitions

Closed circuit television system (CCTV) – is the use of video cameras to transmit a signal to a specific place, for monitoring and recording.

Critical Facility – Area within [COMPANY NAME] facilities with a defined physical security perimeter subject to the NERC Standard CIP-014.

[Other Definitions] – As appropriate or necessary in support of the Security Plan.

General

All persons with unescorted access to [COMPANY NAME] Critical Facilities must be cleared and screened in accordance with [COMPANY NAME] employee and contractor personnel risk assessment screening procedures.

All employees, contractors and security staff must be observant of unusual activities on or around [COMPANY NAME] Critical Facilities.

Anyone arriving with an unidentified or unusual object will be questioned, if there is security presence. If necessary, visual confirmation will be performed. Access to the facility will be denied should the individual refuse inspection. Management will be advised and will give direction for what action will be performed. Security should be notified to report all unusual behavior near this facility.

R5 Physical Security Plan

"Each Transmission Owner that identified a Transmission station, Transmission substation, or primary Control Center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary Control Center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

> 5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
>
> 5.2. Law enforcement contact and coordination information.
>
> 5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
>
> 5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary Control Center(s)."

[COMPANY NAME] shall document, develop, implement and maintain a physical security plan, approved by a member of senior management (CIP-014 R5).

[COMPANY NAME] shall develop the plan(s) within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified within this plan (CIP-014 R5).

The following facility(ies) is/are defined as a Critical Facility, according to Requirement 1 (CIP-014 R5):

Transmission Station, Transmission Substation or Primary Control Center:

[FACILITY NAME]

Security systems will be continually monitored, to detect physical intrusion attempts and or physical attacks.

Access control to the [COMPANY NAME] Critical Facility will be maintained at all times.

This plan is based on security measures/systems currently in place or planned to be deployed. The plan is a living document and will be revised or updated within thirty (30) calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the facility perimeter, physical access controls, monitoring controls; or measures to deter, detect, delay, assess, communicate or respond. It shall also be modified, when there is a change in the threat(s) to the facility.

At a minimum, the plan will be reviewed annually by the [POSITION TITLE] and then approved by senior management.

R5.1 Resiliency or Security Measures

The following physical threats and vulnerabilities, for this facility, were identified during the evaluation conducted in Requirement R4 and the following security measures shall be collectively deployed and implemented to provide protection in depth and mitigate the identified threats and vulnerabilities.

[THREAT #1]
[THREAT #2]
[THREAT #3]
[THREAT #4]
[THREAT #5]
[THREAT #6]

[VULNERABILITY #1]

[THREAT/TACTIC #1]
[THREAT/TACTIC #2]
[THREAT/TACTIC #3]

Deterrence Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Detection Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Delay Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Assessment Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

Communication Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Response Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

[VULNERABILITY #2]
[THREAT/TACTIC #1]
[THREAT/TACTIC #2]
[THREAT/TACTIC #3]

Deterrence Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Detection Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Delay Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Assessment Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Communication Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Response Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

[VULNERABILITY #3]
[THREAT/TACTIC #1]
[THREAT/TACTIC #2]
[THREAT/TACTIC #3]

Deterrence Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Detection Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

Delay Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Assessment Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Communication Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Response Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

[VULNERABILITY #4]
[THREAT/TACTIC #1]
[THREAT/TACTIC #2]
[THREAT/TACTIC #3]

Deterrence Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Detection Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Delay Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Assessment Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Communication Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Response Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

[VULNERABILITY #5]
[THREAT/TACTIC #1]
[THREAT/TACTIC #2]
[THREAT/TACTIC #3]

Deterrence Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Detection Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Delay Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Assessment Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Communication Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]
Response Measures
[MEASURE #1]
[MEASURE #2]
[MEASURE #3]

R5.2 Law Enforcement Contact and Coordination

Local Law Enforcement
[CONTACT #1]
[CONTACT #2]
[CONTACT #3]

County Law Enforcement
[CONTACT #1]
[CONTACT #2]
[CONTACT #3]

State Law Enforcement
[CONTACT #1]
[CONTACT #2]
[CONTACT #3]
Federal/Military
[CONTACT #1]
[CONTACT #2]
[CONTACT #3]

Fire/Medical
[CONTACT #1]
[CONTACT #2]
[CONTACT #3]

Telephone, email or face-to-face meetings, with each of the above contacts, to develop and maintain partnerships for current threat information and alarm response should be made on a scheduled, recurring basis throughout the year. Site tours and training of local First Responders/law enforcement will be deployed when resources are available and the responders/law enforcement are willing.

5.3. Timeline

The following security measures shall be deployed and implemented within [INSERT MAXIMUM TIME] of the publication date of this plan.

Security Measure	Estimated In-Service Date

Resiliency Measure	Estimated In-Service Date

5.4. Provisions to Evaluate Evolving Physical Threats

Potential evolving threats to this facility will be gathered through scheduled, recurring contact throughout the year from the following sources:

[LOCAL INTELLIGENCE SOURCE/S]
[FUSION CENTER/S]
[LOCAL DHS PSA]
[ES-ISAC]
[NERC]
[OTHER U.S. FEDERAL AND/OR CANADIAN, STATE GOVERNMENTAL AGENCIES]

Security measures for this facility may be modified based on a change in threat.

Appendix A – Facility Site Map

Section 5 Physical Security Technologies & Resources

The following are physical security technologies and resources that organizations may consider utilizing; however, each organization should conduct its due diligence to investigate and assess the applicable technology before its implementation.

Compact Surveillance Radar

Compact surveillance radars are small, lightweight radar systems that have a wide coverage area and are able to track people and vehicles in range and azimuth angle. They weigh less than 10 pounds, consume less than 15 watts of power, and are easily deployed in large numbers.

Compact surveillance radar have the same characteristics of the larger ground surveillance radar (GSR), namely the ability to track many moving targets simultaneously, use in all weather, day and night operation, wide coverage areas, and the ability to track targets and cue cameras automatically.

Fiber-Optic Intrusion Detection Systems (FOIDS)

Fiber-optic intrusion detection systems (FOIDS) offer distinct advantages, since they are immune to EMI, RFI, and lightning. Perimeter intrusion detection security systems are based on the core principle of establishing a steady background state and continuously monitoring to detect any change above or below a pre-determined threshold. Changes above or below these thresholds indicates that an intrusion has occurred. To accomplish this, many technologies have been developed and each offers a different method to protect a fence. Fiber-optic fence security systems use light to detect intruders. During operation, light pulses are transmitted through the fiber-optic cable. These light pulses are continuously monitored for any changes in light pattern or optical power, as would occur when the fiber is physically disturbed during an intrusion attempt. For high-security facilities, there is a documented need for high probability of detection and low false/nuisance alarm rates, and it mandates the use of sensors that have tuneable thresholds. Fiber-optic sensors use multiple criteria in conjunction with a tuneable decision network to distinguish between environmental noise and intrusions. Without tuneable thresholds, sensors are unlikely to have the high sensitivity that is required to catch intruders, while keeping false/nuisance alarms sufficiently low.

Ground Based Seismic Detection

These systems can protect fenced and unfenced assets, ranging from an acre in size, such as an electrical substation, to linear assets thousands of miles long, such as a pipeline, by detecting and alerting on threats as they approach.

Algorithms decode ground vibrations, providing an intelligence that automatically and in real-time detects, classifies, locates, and reports on threats. The system is buried and combines a proprietary vibration sensor with a sophisticated suite of detection and classification algorithms. Line of sight to an intruder is not required, allowing a threat to be obscured by weather, darkness, topography, vegetation, or infrastructure and yet still be detected and classified. Because the sensors are buried, they are invisible to intruders.

Gunshot Detection Systems

A gunfire locator or gunshot detection system is a system that detects and conveys the location of gunfire or other weapon fire typically using triangulation of data obtained from acoustic, optical, or other types of sensors, as well as a combination of such sensors. These systems are used by law enforcement, security, military, and businesses

to identify the source and, in some cases, the direction of gunfire and/or the type of weapon fired. Most systems possess three main components:

- An array of microphones or sensors either co-located or geographically dispersed
- A processing unit
- A user interface that displays gunfire alerts

Systems used in urban settings integrate a geographic information system so the display includes a map and address location of each incident.

Infrared Motion Sensors

Passive infrared (PIR) sensors detect changes in the amount of infrared radiation impinging upon it, which varies depending on the temperature and surface characteristics of the objects in front of the sensor. When an object, such as a human, passes in front of the background, the temperature at that point in the sensor's field of view will rise from room temperature to body temperature, and then back again. The sensor converts the resulting change in the incoming infrared radiation into a change in the output voltage, and this triggers the detection. Moving objects of similar temperature to the background but different surface characteristics may also have a different infrared emission pattern, and thus sometimes trigger the detector.

PIRs come in many configurations for a wide variety of applications. The most common models have numerous Fresnel lenses or mirror segments, an effective range of about 30 feet, and a field of view less than 180 degrees. Models with wider fields of view, including 360 degrees, are available—typically designed to mount on a ceiling. Some larger PIRs are made with single segment mirrors and can sense changes in infrared energy over 100 feet away from the PIR. There are also PIRs designed with reversible orientation mirrors, which allow either broad coverage or very narrow “curtain” coverage, or with individually selectable segments to "shape" the coverage.

Infrared Photo Beams

Compared with PIR motion sensors, the infrared beam sensor has the advantage of pet-immunity, low-false alarm rate, as well as weatherproof and non-sensitive to changes of temperature. The infrared beam sensors are widely used for the perimeter protection of security from residential to commercial. Infrared beam sensors adopt the active infrared technology. It consists of a transmitter and receiver. The transmitter and receiver are installed opposite each other. When the infrared beams are interrupted, the detector will set off the alarm. Utilizing multi-beams provides these detectors with the immunity for the pets and small animals.

Perimeter Intrusion Detection Systems (PIDS)

Perimeter Intrusion detection security systems are based on the core principle of establishing a steady background state and continuously monitoring to detect any change above or below a pre-determined threshold. Changes above or below these thresholds indicates that an intrusion has occurred. To accomplish this, many technologies have been developed and each offers a different method to protect a fence.

Perimeter security exists to deter, detect, assess, delay, and respond to an attempted intrusion. When specifying a security technology system, each facility has unique characteristics and security requirements, and should be designed to suit the requirements of each site. Site layouts, facility building locations, the terrain and surrounding environment, the local weather conditions, the presence of trees or other

natural or man-made surroundings, the condition of the fence, and the movement of vehicles in and out of the facility all must be considered.

Electronic Access Control Systems

Access Control Card Readers – Used in physical security systems to read a credential that allows access through access control points, typically a locked door. An access control reader can be a magnetic stripe reader, a bar code reader, a proximity reader, a smart card reader, or a biometric reader. Access control readers are classified by functions they are able to perform and by identification technology.

Barcode – A barcode is a series of alternating dark and light stripes that are read by an optical scanner. The organization and width of the lines is determined by the bar code protocol selected. There are many different protocols. Sometimes the digits represented by the dark and light bars are also printed to allow people to read the number without an optical reader. The advantage of using barcode technology is that it is cheap and easy to generate the credential and it can easily be applied to cards or other items. However, the same affordability and simplicity makes the technology susceptible to fraud, because fake barcodes can also be created cheaply and easily, for example by photocopying real ones. One attempt to reduce fraud is to print the barcode using carbon-based ink, and then cover the bar code with a dark red overlay. The barcode can then be read with an optical reader tuned to the infrared spectrum, but cannot easily be copied by a copy machine. This does not address the ease with which barcode numbers can be generated from a computer using almost any printer.

Biometric – There are several forms of biometric identification employed in access control: fingerprint, hand geometry, iris, and facial recognition. Biometric technology has been promoted for its ability to significantly increase the security level of systems. Proponents claim that the technology eliminates such problems as lost, stolen, or loaned ID cards and forgotten PIN.

All biometric readers work similarly, by comparing the template stored in memory to the scan obtained during the process of identification. If there is a high enough degree of probability that the template in the memory is compatible with the live scan (the scan belongs to the authorized person), the ID number of that person is sent to a control panel. The control panel then checks the permission level of the user and determines whether access should be allowed. The communication between the reader and the control panel is usually transmitted using the industry standard Wiegand interface. The only exception is the intelligent biometric reader, which does not require any panels and directly controls all door hardware.

Biometric templates may be stored in the memory of readers, limiting the number of users by the reader memory size (there are reader models that have been manufactured with a storage capacity of up to 50,000 templates). User templates may also be stored in the memory of the smart card, thereby removing all limits to the number of system users (finger-only identification is not possible with this technology), or a central server PC can act as the template host. For systems where a central server is employed, known as "server-based verification," readers first read the biometric data of the user and then forward it to the main computer for processing. Server-based systems support a large number of users but are dependent on the reliability of the central server, as well as communication lines.

The two possible modes of operation of a biometric reader are 1-to-1 and 1-to-many:

In the 1-to-1 mode, a user must first either present an ID card or enter a PIN. The reader then looks up the template of the corresponding user in the database and compares it

with the live scan. The 1-to-1 method is considered more secure and is generally faster, as the reader needs to perform only one comparison. Most 1-to-1 biometric readers are "dual-technology" readers: they have a built-in proximity, smart card, or keypad reader, or they have an input for connecting an external card reader.

In the 1-to-many mode, a user presents biometric data such as a fingerprint or retina scan, and the reader then compares the live scan to all the templates stored in the memory. This method is preferred by most end-users, because it eliminates the need to carry ID cards or use PINs. On the other hand, this method is slower because the reader may have to perform thousands of comparison operations until it finds the match. An important technical characteristic of a 1-to-many reader is the number of comparisons that can be performed in one second, which is considered the maximum time that users can wait at a door without noticing a delay. Currently most 1-to-many readers are capable of performing 2,000–3,000 matching operations per second.

Magnetic Stripe – A technology, usually called mag-stripe, is named this because of the stripe of magnetic oxide tape that is laminated on a card. There are three tracks of data on the magnetic stripe. Typically, the data on each of the tracks follows a specific encoding standard, but it is possible to encode any format on any track. A mag-stripe card is cheap compared to other card technologies and is easy to program. The magnetic stripe holds more data than a barcode can in the same space. While a mag-stripe is more difficult to generate than a bar code, the technology for reading and encoding data on a mag-stripe is widespread and easy to acquire. Magnetic stripe technology is also susceptible to misreads, card wear, and data corruption. These cards are also susceptible to some forms of skimming, where external devices are placed over the reader to intercept the data read.

Wiegand Card – A patented technology using embedded ferromagnetic wires strategically positioned to create a unique pattern that generates the identification number. Like magnetic stripe or barcode technology, this card must be swiped through a reader to be read. Unlike the other technologies, the identification media is embedded in the card and not susceptible to wear. This technology once gained popularity because it is difficult to duplicate, creating a high perception of security. Proximity cards are replacing this technology; however, because of the limited source of supply, the relatively better tamper resistance of proximity readers, and the convenience of the touchless functionality in proximity readers.

Proximity Card – Proximity card readers are still referred to as "Wiegand output readers," but no longer use the Wiegand effect. Proximity technology retains the Wiegand upstream data, so that the new readers are compatible with old systems. A reader radiates a 1" to 20" electrical field around itself. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil, which transmits it to the reader.

A common proximity format is 26-bit Wiegand. This format uses a facility code, sometimes also called a site code. The facility code is a unique number common to all of the cards in a particular set. The idea is that an organization will have its own facility code and a set of numbered cards incrementing from one. Another organization has a different facility code and its card set increments from one. Thus, different organizations can have card sets with the same card numbers but since the facility codes differ, the cards only work at one organization. This idea worked early in the technology; but as there is no governing body controlling card numbers, different manufacturers can supply cards with identical facility codes and identical card numbers to different organizations. Thus, there may be duplicate cards that allow access to

multiple facilities in one area. To counteract this problem some manufacturers have created formats beyond 26-bit Wiegand that they control and issue to organizations.

In the 26-bit Wiegand format, bit 1 is an even parity bit. Bits 2–9 are a facility code. Bits 10–25 are the card number. Bit 26 is an odd parity bit. Other formats have a similar structure of a leading facility code followed by the card number and including parity bits for error checking, such as the 1/12/12/1 format used by some American access control companies. The 1/8/16/1 format gives a facility code limit of 255 and 65535 card number. The 1/12/12/1 format gives a facility code limit of 4095 and 4095 card number. Wiegand was also stretched to 34 bits, 56 bits, and many others.

Smart Card – There are two types of smart cards: contact and contactless. Both have an embedded microprocessor and memory. The smart card differs from the proximity card in that the microchip in the proximity card has only one function: to provide the reader with the card's identification number. The processor on the smart card has an embedded operating system and can handle multiple applications such as a cash card, a pre-paid membership card, or an access control card.

The difference between the two types of smart cards is the manner with which the microprocessor on the card communicates with the outside world. A contact smart card has eight contact points, which must physically touch the contacts on the reader to convey information between them. Since contact cards must be inserted into readers carefully and in the proper orientation, the speed and convenience of such a transaction is not acceptable for most access control applications. The use of contact smart cards as physical access control is limited mostly to parking applications when payment data is stored in card memory, and when the speed of transactions is not as important.

A contactless smart card uses the same radio-based technology as the proximity card, with the exception of the frequency band used. It uses a higher frequency (13.56 MHz instead of 125 kHz), which allows the transfer of more data and communication with several cards at the same time. A contactless card does not have to touch the reader or even be taken out of a wallet or purse. Most access control systems only read serial numbers of contactless smart cards and do not utilize the available memory. Card memory may be used for storing biometric data (i.e., fingerprint template) of a user. In such case, a biometric reader first reads the template on the card and then compares it to the finger (hand, eye, etc.) presented by the user. In this way, biometric data of users does not have to be distributed and stored in the memory of controllers or readers, which simplifies the system and reduces memory requirements.

Video and Analytics

Video – Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need security monitoring.

CCTV equipment may be used to observe areas from a central control room. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing digital video recorders (DVRs), provides recording, with a variety of quality and performance options and extra features (such as motion detection and email alerts). More recently, decentralized IP cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for completely standalone operation.

Video Analytics – A system using video analytics can recognize changes in the environment and even identify and compare objects in the database using size, speed, and sometimes color. The camera's actions can be programmed based on what it is "seeing." For example, an alarm can be issued if an object has moved in a certain area, is advancing or if an item is missing. IT may also alarm for video loss, lens covering, and other camera-tampering events.

Analytics can also be used to detect unusual patterns in an environment. The system can be set to detect anomalies in a crowd, for instance a person moving in the opposite direction in airports where passengers are only supposed to walk in one direction out of a plane, or in a subway where people are not supposed to exit through the entrances.

Analytics can track people on a map by calculating their position from the images. It is then possible to link many cameras and track a person through an entire building or area. This can allow a person to be followed without having to analyze many hours of film.

Retention, storage and preservation – Most CCTV systems record and store digital video and images to a digital video recorder (DVR) or in the case of IP cameras directly to a server, either on-site or offsite. The amount of data stored and the retention period of the video or pictures are subject to compression ratios, images stored per second, image size, and duration of image retention before being overwritten. Recordings are usually kept for a preset amount of time and then automatically archived, overwritten, or deleted. Videos are kept in order to allow retrieval and review in the event of an incident, a crime, or any number of other reasons.

Many DVRs for CCTV store their contents in a proprietary file format, and export the video files to an optical storage media such as digital versatile disc. When the DVR is damaged before export, a proprietary format hinders recovery of video files and timestamps from a DVR hard disk in a forensically sound manner.

IP cameras – A growing format in CCTV is internet protocol cameras (IP cameras). IP cameras use the IP within most local area networks (LANs) to transmit video across data networks in digital form. IP can optionally be transmitted across the public Internet, allowing users to view their cameras through any Internet connection available through a computer, smart phone, or other mobile device. For professional or public infrastructure security applications, IP video should be restricted to within a private network, VPN, or can be recorded onto a remote server.

HD Video – An increasing number of manufacturers of security cameras now offer HD cameras. The need for high resolution, color fidelity, and frame rate is acute for surveillance purposes to ensure that the quality of the video output is of an acceptable standard that can be used both for preventative surveillance as well as for evidence purposes. These needs, however, must be balanced against the additional storage capacity required by HD video.

Integrated VMS (Video Management Systems) **–** Software provides remote video monitoring, recording, and event management functionality. Its API allows the integration with other systems such as alarm inputs and access control.

Appendix 1 – Additional Resources

ASIS Facilities Physical Security Measures 2009 (https://www.asisonline.org/Standards-Guidelines/Guidelines/published/Pages/Facilities-Physical-Security-Measures-Guideline.aspx)

ASIS Security Management Standard: Physical Asset Protection 2012 (https://www.asisonline.org/Standards-Guidelines/Standards/published/Pages/Security-Management-Standard-Physical-Asset-Protection.aspx)

DHS Energy Sector – Specific Plan, An Annex to the National Infrastructure Protection Plan 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf)

IEEE 1402, Guide for Electric Power Substation Physical and Electronic Security (https://standards.ieee.org/findstds/standard/1402-2000.html)

IES, The Lighting Handbook, 10th Edition (https://www.ies.org/handbook/)

NERC Security Guideline for the Electricity Sector: Physical Security 2012 (http://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202012-05-18-Final.pdf)

NERC Security Guideline for the Electricity Sub-sector: Physical Security Response 2013 (http://www.nerc.com/docs/cip/sgwg/Physical_Security_Guideline_2012_01_05_V1_9_45_day_review.pdf)