

## IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS

Date: \_\_\_\_\_ Facility \_\_\_\_\_

### Information on

This checklist identifies the physical security elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Physical Security Elements	Element Present		Comments
	Yes	No	
Security Program Management			
Threat Detection and Evaluation Capabilities			
Perimeter Barriers			
Access Controls			
Building Barriers			
Intrusion Detection			
Lighting			
Closed Circuit Television (CCTV)			
Signage			
Security Force			
Human Resources Security Procedures			
Protection of Sensitive Security Information			

## SECURITY PROGRAM MANAGEMENT

<b>(a) Security Organization</b>	
<p>1. Is there a senior level security working group with representatives from each major department to establish security policies (including physical security, operations security, and infrastructure interdependencies security) and integrate them across all elements of the organization? • If yes, describe the membership, the lines of communication, and any scheduled periodic meetings. • If there is not such a group, how are security policies established?</p>	
<p>2. Is there a security office that is responsible for implementing security policies and procedures (including physical security, operations security, and infrastructure interdependencies security)? • If yes, where does it report in the organization, how many people are in the office, and are resources adequate? Also describe any training received. • If there is not such an office, how are security policies implemented?</p>	

  

<b>(b) Security Plans and Policies</b>	
<p>1. Is there a mission statement describing the physical security, operations security, and infrastructure security programs?</p>	
<p>2. Is there a formal security plan and statement of security policies? If there is, describe it including how it is communicated to employees.</p>	

  

<b>(c) Security Resources</b>	
<p>1. Are the resources (budget and staff) applied to security (including physical security, operations security, and infrastructure interdependencies security) considered adequate?</p>	
<p>2. Do security personnel feel that they have adequate training to accomplish their functions?</p>	

**(d) Security Audits**

1. Is there a regular security assessment or audit conducted of the facility or critical asset? If yes, describe how it is done, by whom, and how frequently.

2. Has the most recent audit indicated any weaknesses? Summarize the results of the audit, particularly any weaknesses identified.

3. Have any corrective measures been implemented recently? Describe them.

**(e) Internal Communications**

1. Is the company able to ensure that company personnel can respond to alarms, outages, or other issues at critical operating facilities?

2. Is there a system of communicating threat warnings to appropriate organizations within the company along with appropriate actions to implement based upon the declared threat level?

3. Are security related incidents promptly reported within the company as well as to local enforcement agencies?

(Those incidents falling within the NERC threat-reporting guidelines should also be reported promptly to the National Infrastructure Protection Center (NIPC) and the ES-ISAC

4. Has the company established an effective liaison relationship with its local offices of federal, regional, and local law enforcement agencies, especially in the areas where critical facilities are located?

(Where feasible, provide familiarization tours for law enforcement agencies having jurisdiction in areas where critical facilities are located, and conduct pre-planning and coordination for potential response scenarios. This liaison should be periodically updated and verified to ensure that contact information and facility familiarization is current).

<p>5. Has the company established contact with (for example) the Key Asset Program Coordinator or InfraGard Coordinator of the FBI Division Headquarters for the service territory?</p> <p>(Note: In large geographic areas or for companies operating in multiple states, several FBI Divisions may need to be contacted).</p>	
<p>6. Has the company developed liaison with officials having regional mutual aid jurisdiction (generally the Sheriff's Department) and any regional law enforcement groups that represent multi-agency coordination as well as with the local law enforcement agencies having direct jurisdiction near critical facilities?</p>	
<p>7. Has the company provided preplanning familiarization tours of critical sites to law enforcement?</p>	
<p>8. Has the company established single points of contact?</p> <p>(Ideally, these should be 24/7 contact numbers (e.g. security control centers, dispatch centers, pagers, etc. Where companies operate in multiple states, local contacts may be preferable, but single points of contact tend to ensure more timely and consistent dissemination of information within companies).</p>	
<p>9. Describe the process for obtaining feedback from employees on security related issues.</p>	

(f) Vulnerability and Risk Assessment	
<p>1. Has a process been developed to identify critical electric infrastructure systems and facilities both from a physical and cyber security perspective?</p>	
<p>2. Have security response requirements been coordinated with law enforcement officials at the appropriate local, regional, and federal levels to assure good communication and coordination?</p>	
<p>3. Is there an emergency management response process to reduce or mitigate impacts of a loss of electric supply or deliverability?</p>	

<p>4. Are there formal mutual assistance agreements at the appropriate local, state, or regional level to support response, repair and restoration activities for the disrupted facility?</p> <p>(Consider interdependencies among infrastructures when evaluating the consequences of a cyber or physical security incident. An incident in one infrastructure can cascade to failure in other infrastructures).</p>	
---	--

<b>(g) Emergency Plans</b>	
<p>1. Are there formal mutual assistance agreements which include notification of law enforcement and state emergency preparedness officials in place?</p>	
<p>2. Are there contingency plans that are appropriate and flexible for addressing incidents at system control centers, critical substations, and generation stations in place?</p>	
<p>3. Is there a formal and defined emergency management process to mitigate physical and cyber security incidents and restore service quickly? (Plans should include the identification, procurement, and proper security for critical spare parts).</p>	
<p>4. Is there notification process for employees, contractors, and vendors? (Well informed personnel are a company's first line of defense for observing and reporting suspicious activities in and around their facilities or their information technology (IT) systems.</p>	
<p>5. Are there emergency preparedness plans that address cyber and physical security counter measures when threat information is received from the NIPC, ES-ISAC, or other agencies?</p>	

<p>6. Is there a training and orientation program for key responders? (Should be developed and periodically reviewed. Periodic exercises may include tabletops with stretching scenarios and include first responders from law enforcement, fire, and state authorities when appropriated).</p>	
---	--

**(h) Emergency Operations Center**

<p>1. Is there standby power as well as sufficient information and communication infrastructure to support emergency operations?</p>	
<p>2. Are there sufficient resources to manage an emergency including clerical support, operating diagrams, manuals, and other reference materials?</p>	
<p>3. Is there a person designated as responsible for the update and maintenance of the emergency center and its alternate?</p>	
<p>4. Has the company designated an Emergency Management Team (EMT)? The team should have representation from the following:</p> <ul style="list-style-type: none"> <li>a. Operations (Generation, Transmission, Distribution).</li> <li>b. External Communications (External Relations, Customer Services, Call Center Operations, Human Resources, and others).</li> <li>c. Logistics (Facilities, Materials, IT Support, etc.).</li> <li>d. Finance (Controller, Banking, etc.)</li> <li>e. Security.</li> <li>f. Information Technology</li> </ul>	

**(i) Continuity of Business Processes**

<p>1. Is there a business recovery plan that identifies the key functions that may need to be</p>	
---	--

relocated, an alternate work location for each critical function, and the resources needed to ensure their continued operation at a minimum acceptable level?	
2. Are there plans for relocating critical operations such as their Grid Control Center, Data Center, Customer Call Center, and other key operating facilities?	
3. Are the alternate facilities for these functions located sufficiently distant from the primary location to ensure rapid continuity of operations?	
4. Are the alternate facilities able to maintain critical operation at some minimal level until the primary facility is restored?	
5. Has a person or department been designated to develop, maintain, and test the business recovery plan?	
6. Are there specific emergency plans for individual critical functions that supplement the overall business recovery plan?	
7. Are there protocols for the activation of the business recovery plan including facility preparation, systems activation, and relocation of personnel?	
8. Are there annual tests of the business recovery plan? Is a review of lessons learned conducted? How are revisions implemented into the plan?	
9. Is there training for key personnel to ensure that they are aware of the business recovery plan requirements?	

**(j) Protecting Potentially Sensitive Information**

<p>Are there information security or confidentiality policies in place as an integral part of the company's business level policies?</p> <p>(The policy should address the production, storage, transmission, and disposal of both physical and electronic information. The policy should define the hierarchical confidentiality classification framework (e.g. Public, Market Participant Confidential, Company Confidential, Highly Confidential) as well as the authorization requirements and conditions to permit disclosure).</p>	
<p>2. Is there a designated single person or department responsible for reviewing all third party requests for sensitive information and, in particular, reviewing information placed in the public domain?</p> <p>(That department will generally have to coordinate closely with the company's legal counsel).</p>	
<p>3. Is there a process in place to respond to disclosures of sensitive information to ensure that they are addressed promptly and appropriately?</p> <p>(This process should include informing and involving senior management, market participants, government, regulators, law enforcement, the public and the media, as appropriate).</p>	
<p>4. Is there an ongoing employee awareness training program to ensure that information is appropriately secured?</p>	
<p>5. How is sensitive information identified and marked?</p>	
<p>6. Who has access to sensitive security information?</p>	

7. How is sensitive information protected, stored, accessed, transmitted, and destroyed?	
8. How do senior executives/managers protect sensitive security information?	

## THREAT DETECTION AND EVALUATION CAPABILITIES

<b>(a) Threat Analysis Working Group</b>	
1. Is the organization a member of a local threat analysis working group? Describe the group	
2. If the organization is a member of such a group, list the organizations that participate in the working group (e.g., local, county, state, and federal agencies, the military).	
3. Do the participants in the working group have management support, requirements, and funding to participate? Describe the situation.	
4. Do the members of the working group have the authority to share information with other members of the group? Describe the situation.	
5. Have the members of the working group been given U.S. government clearances to share in threat information? Describe the situation.	
6. Do the members of the working group have access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc., (ANSER), FBI-sponsored InfraGuard, and other information system security warning notices? List the threat information systems they use.	
7. Indicate the frequency and regularity of the working group meetings.	
8. Do the members of the working group have processes in place to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses)? Describe these processes.	
9. Do some members of the working group conduct scheduled meetings with the public to discuss concerns and observations? Describe these interactions.	

<p>10. Do the members of the working group understand industry interdependencies and work with other industry members to address these potential concerns? Describe the extent of these interactions.</p>	
<p>11. What are the roles and responsibilities of the working group members during response and recovery activities?</p>	

**(b) Organization's Response to Threat Updates**

<p>1. Does senior management support and/or participate in the threat analysis working group? Describe the extent of the support/ participation.</p>	
<p>2. Does the organization receive as-needed threat briefings from local, state, and federal agencies? Describe the nature and extent of the briefings.</p>	
<p>3. Does the organization have the ability to distribute organization-specific threat warnings in real time? Describe the process.</p>	
<p>4. Does the organization have the ability to augment security programs based on threat updates? Describe the process.</p>	
<p>5. Does the organization conduct historical trending analysis for security events (both planned and actual) and implement security activates to mitigate them? Describe the analysis.</p>	
<p>6. Does the organization create possible threat scenarios based on input from the threat analysis working group and conduct related security exercises? Describe the exercises.</p>	

## PERIMETER BARRIERS (FENCES, GATES)

<b>(a) Fences</b>	
<p>1. Fence construction rating:</p> <p><u>Low</u>: No fence/fence less than 6-foot high.</p> <p><u>Moderate</u>: 6-foot chain-link fence with outriggers.</p> <p><u>High</u>: 8-foot (or higher) chain-link fence with outriggers.</p> <p><u>Other</u>:</p>	
<p>2. Does the bottom of the fence fabric extend to within 2 inches of firm ground? Are surfaces stabilized in areas where loose sand, shifting soils, or surface waters may cause erosion and assist an intruder in penetrating the area?</p>	
<p>3. Where surface stabilization is not possible or practicable, are concrete curbs, sills, or other similar type anchoring devices, extending below ground level provided?</p>	
<p>4. Are posts, bracing's, and other structural members located on the inside of the fence fabric? Are galvanized steel 11 or aluminum tie-wires equal in gauge to fencing used to secure the fence fabric to posts and other structural members?</p>	
<p>5. If practicable, do clear zones extend 12 feet on the outside and 30 feet on the inside of the perimeter fence? Are clear zones free of all obstacles, topographical features, and vegetation exceeding 8 inches in height which reduce the effectiveness of the physical barrier, impede observation, or provide cover and concealment of an intruder?</p>	
<p>6. Are drainage structures and water passages penetrating the barrier barred to provide penetration resistance equivalent to the fence itself? Are openings to the drainage structures having a cross-sectional area greater than 96 square inches, and a smallest dimension greater than 6 inches protected by securely fastened welded bar grills.</p>	

7. Is the fence protected from vehicles? (specify).	
8. Is the fence alarmed? If yes, describe sensor type(s).	

<b>(b) Gates</b>	
1. Characterize gate construction: (specify).	

2. Are the gates structurally comparable (provide penetration resistance) equivalent to the adjacent fence?	
3. Is the number of vehicular and pedestrian gates along the perimeter kept to a minimum? (consider operational requirements)	
4. Unless manned 24 hours a day, are the gates provided with an approved lock? Are the hinge pins and hardware welded or otherwise modified to prevent easy removal?	
5. How is access to gate keys controlled?	

<b>(c) Vehicle Barriers</b>	
1. Are vehicle barriers utilized? If yes specify type/operation.	

--	--

## ACCESS CONTROL

<b>(a) Personnel Access</b>	
1. Access point control: Unmanned, unarmed guard, armed guard, or other (specify).	
2. To the extent allowed by state and local law, is access to the facility limited to employees or other individuals with a valid need to enter the premises? Is a record kept of who comes into the facility?	
3. Identification check process: None in place, casual recognition, credential check, or other (describe).	
4. Badging policy: No badging policy, badge issuance and control procedures in place (describe).	
5. Cards and badges identify the area(s) for which they are valid and badges show permission to access specific areas (describe).	
6. Are visitors escorted throughout the building or facility? Describe the nature of the escort. Is access granted only after person can substantiate a legitimate business purpose?	

<b>(b) Vehicle Access</b>	
1. Vehicle access point: Describe as unmanned, unarmed guard, armed guard, or other.	

<p>2. Vehicle access control process: None in place, vehicle stickers, vehicle stickers with personnel identification, automated system, or other (specify).</p>	
<p>3. Are there vehicle screening procedures in place? Describe as none, cursory, or detailed</p>	
<p>4. Are vehicle deliveries pre-scheduled? Is a list of drivers/deliveries provided prior to delivery?</p>	
<p>5. Have distinct delivery areas been designated for receiving and screening packages prior to their distribution within the facility? Are there established procedures to screen packages to determine if they should be distributed as addressed or held at the delivery area for further scrutiny?</p>	
<p>6. Is parking of private vehicles allowed near buildings and other structures? Are employee and visitor vehicles prohibited from a parking in secure areas?</p>	
<p>7. Are utility vehicles locked and parked in an area within the facility perimeter.</p>	

**CONSTRUCTION STANDARDS (WALLS, ROOF/CEILING, WINDOWS, DOORS)  
FOR BUILDINGS/AREAS CONTAINING SENSITIVE INFORMATION AND ASSETS**

<b>(a) Walls</b>	
<p>1. Characterize wall construction and rate the level of security provided:</p> <p><u>Low</u>: chain-link mesh, 16-gauge metal, wood studs and dry wall, wood studs and plywood, or other (specify).</p> <p><u>Moderate</u>: clay block, 8-inch hollow block, 8-inch filled block, or other (specify).</p> <p><u>High</u>: 8-inch filled rebar block, 12-inch filled rebar block, 2-inch precast concrete tees, 4-inch reinforced concrete, 8-inch reinforced concrete, 12-inch reinforced concrete, 24-inch reinforced concrete</p> <p><u>Other</u>: (specify).</p>	
<p>2. If building walls are incorporated into the barrier system, do they provide penetration resistance equivalent to the perimeter barrier and are subject to observation?</p>	
<p>3. Do the walls extend from the floor to the structural ceiling?</p>	

--	--

**(b) Roof/Ceiling**

<p>1. Characterize the roof material and rate the level of security it provides:</p> <p><u>Low</u>: 20-gauge metal with insulation, ½inch wood, or other (specify).</p> <p><u>Moderate</u>: 20-gauge metal built-up roof, concrete built-up roof with T-beams, or other (specify).</p> <p><u>High</u>: 5-1/2-inch concrete roof, 8-inch concrete roof, other (specify)</p>	
<p>2. Are floors, if on grade, a minimum of 6 inches concrete construction reinforced with 6 inches by 6 inches mesh or equivalent bars?</p>	

**(c) Windows**

<p>1. Are windows and other openings sealed with material comparable to that forming the adjacent walls and otherwise limited to the minimum number essential?</p>	
--	--

<p>2. Characterize the window materials and rate the level of security they provide:</p> <p><u>Low:</u> standard windows or other (specify).</p> <p><u>Moderate:</u> 9-gauge expanded mesh, 1/2-inch diameter x 1-1/2-inch quarry screen,</p> <p><u>High:</u> 1/2-inch diameter bars with 6-inch spacing, 3/16-inch x 2-1/2-inch grating</p> <p><u>Other:</u> (specify).</p>	
<p>3. Are there alarms on windows that are accessible by foot or ladder Describe as: None, or by sensor type.</p>	

<b>(d) Doors</b>	
<p>1. Characterize door materials and rate the level of security they provide:</p> <p><u>Low:</u> wood, 9-gauge wire mesh, hollow-core metal, no lock/hinge, or other (specify).</p> <p><u>Moderate:</u> hollow-core metal, tempered-glass panel, security-glass panel, turnstile, or other (specify).</p> <p><u>High:</u> security: ½-inch steel plate, turnstile – aluminum, Class V or VI vault</p> <p><u>Other:</u> (specify).</p>	
<p>2. Are door bucks, frames, and keepers rigidly anchored and provided with anti-spread space filler reinforced to prevent disengagement of the lock bolt by prying or jacking of the door frame?</p> <p>(The frames and locks for both interior and exterior doors should be designed and installed to prevent the removal of the frame facing or the built-in locking mechanism).</p>	
<p>3. Are hinges of the fixed pin security hinge type or equivalent? Are exposed hinge pins pinned, spot welded, or otherwise secured to prevent removal?</p>	

<p>4. Characterize the door locks and rate the level of security they provide:</p> <p><u>Low:</u> No lock, lock not used, or other (specify).</p> <p><u>Moderate:</u> door unlocked, attended by personnel when unlocked, ID actuated lock, padlock, keyed cylinder lock, combination lock, mechanically coded lock, or other (specify).</p> <p><u>High:</u> electronically lock, two-person rule lock system, lock inaccessible from the door exterior</p> <p><u>Other:</u> (specify).</p>	
<p>5. How are keys for the door locks controlled?</p>	
<p>6. Door Alarms: Characterize as: no door alarm; door alarmed (Indicate the type of door sensor). Is door position monitored?</p>	

## INTRUSION DETECTION SYSTEMS (IDS)

<b>(a) Intrusion Detection System (Sensor Type/locations)</b>	
<p>1. Characterize type/locations of exterior intrusion detection sensors. Are the sensors positioned to prevent gaps in coverage? Are detection zones kept clear of obstructions?</p>	
<p>2. Characterize type/locations of interior intrusion detection sensors. Are the sensors positioned to prevent gaps in coverage? Are detection zones kept clear of obstructions?</p>	
<p>3. Are buildings and critical structures alarmed to detect intrusion?</p>	
<b>(b) Intrusion Detection (Monitoring/Response)</b>	
<p>1. Is the IDS system continuously monitored? Are there arrangements in place to ensure a prompt response, in case of unauthorized entry, by law enforcement, private security companies, or a monitoring service?</p>	
<p>2. Is the IDS designed to cause a visual and audible alarm at the central control panel whenever the system is turned off or malfunctions? Are transmission lines for the alarm circuits electrically supervised and dedicated to minimize undetected tampering?</p>	
<p>3. Are only authorized personnel allowed access to IDS installation wiring diagrams for a specific facility or location?</p>	
<p>4. Is the IDS provided with independent, protected, backup power supply that will meet the backup power requirements?</p>	

--	--

## LIGHTING

<b>(a) Lighting</b>	
1. Is the lighting system designed to deny an intruder approaching the area the cover of darkness, and enable personnel at the facility to detect unauthorized personnel within the area?	
2. Is there security lighting for the access points? (describe the lighting system).	
3. Is lighting provided along site perimeter barriers? (describe)	

<p>4. Is there security lighting for the gates (describe lighting system). Do alarms or infrared detectors trigger the lighting? Describe the triggering process.</p>	
<p>5. Is there security lighting for the fences? (describe lighting system).</p>	
<p>6. Are switches for exterior lights installed so that they are not accessible to unauthorized individuals?</p>	
<p>7. Are all exterior lights covered with wire mesh screen that will prevent their being broken by thrown objects? (Vandal resistant lenses may be used instead of wire mesh screen).</p>	
<p>8. Is emergency lighting and standby power available?</p>	
<p>9. Is there night lighting throughout the facility for surveillance?</p>	

## CLOSED CIRCUIT TELEVISION (CCTV)

<b>(a) CCTV</b>	
<p>1. Describe the CCTV system in use at the site. Characterize cameras in use (PTZ, Fixed, Day/Night) and what asset(s) the cameras cover.</p>	
<p>2. Who monitors the CCTV cameras and what are the protocols for camera operation? Is there a protocol to follow when an alarm is received or video surveillance shows an anomaly?.</p>	
<p>3. Do cameras have the capability of being recorded on a 24/7 basis? Is video archived for a minimum of 30 days?</p>	
<p>4. Is the camera monitoring and recording equipment located in a secure area with restricted access?</p>	
<p>5. Is the CCTV system and other monitoring devices connected to an uninterruptible power supply such as an emergency generator with an automatic transfer switch or battery back-up to assure continued operation in a power failure?</p>	
<p>6. Are there overgrowth of trees and shrubs that could prevent surveillance by CCTV?</p>	

7. Is the CCTV equipment maintained in good operating order at all times?	

**SIGNAGE**

<b>(a) Signage</b>	
<p>1. Are signs posted at each entrance or approach to the area, and on perimeter fences or boundaries of the area?</p>	
<p>2. Are critical/sensitive areas within the facility clearly marked to indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security?</p>	

3. Are signs posted visibly, at eye level, (when possible)?	

## SECURITY FORCE

<b>(a) Protective Force</b>	
1. Specify the size of the protective force (total number and the number on duty during working hours, non-working hours, and weekends/holidays).	
2. Describe the organization of the protective force (command structure, mission, standard operating and emergency response procedures).	
3. Describe the equipment available to the protective force (i.e. uniforms; vehicles; weapons; communications devices, etc).	
4. Describe the training of the protective force (initial training, site specific, on-the-job, etc.).	
5. Is there a protective force command and control center? Describe it. Is there a backup center? Describe it.	
6. Are there provisions for a back-up force (e.g., recalling off-duty personnel)? Describe the provisions in place.	
7. Are periodic patrols conducted of facilities and areas used to store sensitive or critical items or equipment?	
8. Are patrol and checks conducted on an irregular basis to avoid establishing a pattern?	

<p>9. Are guard procedures reviewed at least annually, and revised (if necessary) to provide greater application of security measures? Describe protective force procedures for responding to alarms.</p>	
---	--

<b>(b) Local Law Enforcement Agencies</b>	
<p>1. Describe the interaction of the protective force with local law enforcement agencies in terms of memoranda of agreement or other agreements in place (describe), protection responsibilities, communication procedures, and participation in drills and exercises.</p>	
<p>2. What is the approximate response time for local law enforcement personnel?</p>	

## HUMAN RESOURCES SECURITY PROCEDURES

<b>(a) Responsibilities</b>	
<p>What organization(s) is responsible for dealing with security-related personnel issues?</p>	
<b>(b) Background Checks</b>	
<p>1. Are background checks done on employees? If yes, for which employees?</p>	
<p>2. Is the background check done for selected (sensitive) positions? If yes, what are the criteria for identifying sensitive positions?</p>	
<p>3. Do background investigations, when conducted, comply with all applicable federal and state laws such as the Fair Credit Reporting Act?</p>	
<p>4. Do background investigations (full or limited) for applicants who are non-citizens or who have lived outside the country within the last 5 to 7 years require international inquiries including education, criminal, and previous employer checks?</p>	
<p>5. Are pre-employment screening conducted for contractors and vendors who either work at or work in direct support of critical facilities?</p> <p>(The company may require that employment agencies conduct background investigations for contract personnel using the same criteria the company used for prospective employees. An audit of the employment agency screening processes may be included as part of the company's normal contract compliance program)</p>	

<p>6. Has the company designated the department or function responsible for pre-employment screening?</p> <p>(Typically conducted by or coordinated with the company's Security Department).</p>	
<p>7. Is the criteria that will be used to deny employment made known to job applicants?</p> <p>(The questions on the application form and the disqualification criteria should be reviewed and approved by the Human Resources and Legal departments to assure that state and federal laws are complied with)</p>	
<p>8. How extensive are the background checks? Do they vary with the sensitivity of the position?</p>	

<b>(c) Insider Threats</b>	
<p>Are there current conditions in the company that might create a threat from insiders (e.g., low morale, lay-offs, labor disputes)?</p>	
<p>Are there security procedures for handling disgruntled or at-risk employees? If yes, describe.</p>	
<p>What are the security procedures for handling terminated employees? How many have been terminated in the last year? Have there been any security incidents related to a terminated employee?</p>	

<b>(d) Disciplinary Procedures</b>	
<p>What are the policies and procedures for incidents of security concern?</p>	

What are the policies and procedures for other disciplinary actions?	
--	--

<b>(e) Security Training</b>	
Is there a company Security Awareness training program that includes initial and periodic security training? Does it include sections on security contacts, critical assets, threats, sensitive information that needs to be protected, reporting suspicious activities, and employee responsibility?	