## 7.3.7 Technical safeguards - Physical

Provide ratings from 0 to 10 for each item, add up the rates and divide by 15 for the overall rating.

### 7.3.7.1 Time

| *Item* | *Rate* |
|---|---|
| Time to breach is used to define physical defense requirements. | |
| Risk management dictates time to breach requirements. | |
| Detection time for physical attack is determined based on time to breach and time to respond with adequate force. | |
| Response time is determined by detection time and time to breach. | |
| Time is measured against attack graphs to determine force levels. | |
| Adequate forces at distances are available for effective response against identified threats. | |
| Total for this area / 6 | |

### 7.3.7.2 Location

| *Item* | *Rate* |
|---|---|
| Location is used to determine force levels, response times, and threats for physical defense design. | |
| Proximity to natural hazards is considered in physical defense planning. | |
| Earthquakes, tsunamis, volcanoes, hurricanes, tornados, floods, lightning, dust, temperature, wind, and other factors are all considered in location-based defenses. | |
| Perimeters are designed to withstand natural forces at the maximum levels seen over long periods at the location. | |
| Distances for redundancy are determined by the nature of natural disasters associated with location. | |
| Physical defenses are designed to protect against levels of crime, civil unrest, government services, and other location-based situations. | |
| Profile level of space is limited so that high valued systems are placed in low profile locations. | |
| Risk management uses location in determining defensive requirements. | |
| Total for this area / 8 | |

### 7.3.7.3 Paths

| *Item* | *Rate* |
|---|---|
| Paths from threats to targets are used in analysis of attack and defense strategies. | |
| Attack graphs are generated and analyzed over time for individual threats to understand and design defenses. | |
| Topological restrictions are considered based on threat capabilities to bypass topological barriers. | |
| Detection times associated with different attack paths are considered in the analysis of defenses. | |
| Response times based on resulting paths including defended paths are considered in defense design and analysis. | |
| Force levels take path restrictions into account. | |
| Total for this area / 6 | |

### 7.3.7.4 Properties

| *Item* | *Rate* |
|---|---|
| Properties associated with materials used are considered in the design of physical defenses. | |
| Properties of barriers are considered in the design and analysis of defenses. | |
| Entry and exit processes are designed based on desired properties associated with the barriers they bypass. | |
| Time to penetrate, noise levels, detectability, and other properties are considered in defense design and analysis. | |
| Risk management considers properties in their analysis. | |
| Total for this area / 4 | |

### 7.3.7.5 Attack graphs

| *Item* | *Rate* |
|---|---|
| Attack graphs are used to express and analyze the set of sequences of steps in physical attacks. | |
| Step by step analysis of successive barriers between attacker and target and target and escape (if planned) are analyzed for time and capability requirements to plan attack and defense for medium and high risk systems. | |
| Attack graphs are validated and analyzed for time and equipment requirements in order to properly stage and time processes for medium and high risk systems. | |
| Risk management reviews attack graphs to evaluate strategies for high risk systems. | |
| Total for this area / 4 | |

### 7.3.7.6 Entry

| *Item* | *Rate* |
|---|---|
| Normal entry points are analyzed for all physical defenses. | |
| Emergency entry points are analyzed for all physical defenses. | |
| Forced entry is analyzed in all physical defense. | |
| Surreptitious entry is analyzed in all physical defense. | |
| Entry defenses consider who goes in, what they bring with them, if they are allowed, and whether they should be where they are. | |
| Increased surety defenses against entry are used for higher risk systems and facilities. | |
| All entries into medium and high surety areas are logged and verified. | |
| No unauthorized devices may enter high surety areas. | |
| Total for this area / 8 | |

### 7.3.7.7 Egress

| *Item* | *Rate* |
|---|---|
| On exit from medium and high surety areas personnel must check out of the area. | |
| Exists are tracked for medium and high surety areas. | |
| Upon exit, verification is done that the individual previously entered the facility and that the corresponding entry is logged. | |
| Only authorized individuals with written records of removal may remove any device from medium or high surety areas. | |
| Total for this area / 4 | |

### 7.3.7.8 Emergencies

| *Item* | *Rate* |
|---|---|
| Emergency entrances into medium and high surety areas are controlled by special emergency procedures. | |
| Emergency exits from medium and high surety areas go to medium and high surety holding areas for verified facility exit. | |
| Comprehensive emergency plans are in place and practiced to assure that security doesn't break down. | |
| Situations that induce emergencies have adequate audit trails to determine causes and sequences for later analysis. | |
| Surveillance of emergency situations is kept for subsequent analysis. | |
| Total for this area / 5 | |

### 7.3.7.9 Hardening

| *Item* | *Rate* |
|---|---|
| Hardening of physical structures is used to make attacks harder. | |
| Threat assessments are used to determine proper hardening in medium and high risk systems. | |
| Hardening is taken into account in analysis of attack times. | |
| Total for this area / 3 | |

### 7.3.7.10 Locks

| *Item* | *Rate* |
|---|---|
| Keyed, digital, or analog controls of electrical, mechanical, fluid, or gaseous mechanisms that are controlled based on time, location, sequence, and situation are selected based on risk management decisions. | |
| Failsafe features are considered in lock selection. | |
| Default settings are considered in lock selection. | |
| Tamper evident locks are used for high surety areas. | |
| Redundant locking mechanisms are used in medium and high surety areas. | |
| Total for this area / 5 | |

### 7.3.7.11 Mantraps

| *Item* | *Rate* |
|---|---|
| Mantraps are used to protect entry to medium and high risk facilities. | |
| Mantraps are used to protect exit from medium and high risk facilities. | |
| Legal issues are addressed in mantrap design and implementation. | |
| Legal approval is required for all mantraps. | |
| Mantraps have emergency communications and surveillance systems and rapid response capabilities for release. | |
| Total for this area / 5 | |

### 7.3.7.12 Surveillance

| *Item* | *Rate* |
|---|---|
| Surveillance systems include coverage of a range of physical phenomena including but not limited to audio, visual, temperature, humidity, proximity, dew point, pressure, air flow, door and window state, heat, motion, smoke, and chemical presence, absence, and level. | |
| Surveillance systems are monitored 24x7. | |
| Surveillance systems are recorded with recording times set by available capacity and typical review time. | |
| Surveillance recordings are preserved whenever an incident occurs in a nearby or related facility or system. | |
| Surveillance systems are connected to alarm systems. | |
| Surveillance systems generate alarms on out of normal conditions. | |
| Surveillance systems generate alarms on known hazard conditions. | |
| Workers are notified of the presence of surveillance systems. | |
| Surveillance is covered in employee contracts. | |
| Surveillance systems are used in response conditions and record all responses within their viewing range for permanent records. | |
| Networked surveillance systems are protected to a level of surety appropriate to the risk levels they cover. | |
| Surveillance systems are used in coordination with badging and computer-related identification and authorization systems. | |
| Surveillance is used in all non-low risk areas, are regularly tested, and have protection against replay attacks. | |
| Total for this area / 13 | |

### 7.3.7.13 Response time

| *Item* | *Rate* |
|---|---|
| Response time is tuned to mitigation of consequences as defined by risk management requirements. | |
| Location of forces are determined based on response time. | |
| Resourcing for resource forces is based on multiple engagements at a level defined by risk management. | |
| Diversions are considered in response times. | |
| Subversions are considered in response times. | |
| Total for this area / 5 | |

### 7.3.7.14 Force

| *Item* | *Rate* |
|---|---|
| Force levels are based on risk management requirements. | |
| Force levels take into account multiple simultaneous events. | |
| Force levels take into account response times to events. | |
| Force levels take into account threats. | |
| Forces are properly trained, maintained, and led. | |
| Total for this area / 5 | |

### 7.3.7.15 OODA loops

| *Item* | *Rate* |
|---|---|
| OODA loops are used to analyze physical security systems for response times. | |
| Training is used to reduce OODA loop times. | |
| OODA loops are reduced by reducing time to detect. | |
| OODA loops are reduced by rapid triage using real-time remote sensors. | |
| OODA loop times are analyzed for improvement during testing. | |
| Total for this area / 5 | |

### 7.3.7.16 Summary

Using ratings from the sections above, enter results in each area identified. Sum the results and divide by 15 for an overall rating.

| *Area* | *Rate* |
|---|---|
| Time | |
| Location | |
| Paths | |
| Properties | |
| Attack graphs | |
| Entry | |
| Egress | |
| Emergencies | |
| Hardening | |
| Locks | |
| Mantraps | |
| Surveillance | |
| Response time | |
| Force | |
| OODA loops | |
| Total of other totals / 15 | |

| ***Startup*** | ***Diligence*** | ***Typical*** | ***Excellent*** | ***Best*** |
|---|---|---|---|---|
| 2.5 | 5 | 5 | 7 | 9.5 |