

**WORKBOOK 14.2: SECURITY INSPECTION AND VALIDATION (SIV)
CHECKLISTS** 

Purpose: To present a sample security inspection and validation checklist

Security Inspection and Validation Policies and Procedures Checklist

Note: This checklist focuses primarily on the security policies and procedures employed at the facility. When identifying the various aspects of policies and procedures it is important to not only check for their existence, but to ensure that they are being applied as required. Consider the following questions and check the appropriate box for each response.

Question: Policies and Procedures	Yes ✓	No ✓
Do employees wear and visibly display identification cards at all times while in the building?		
Are signs posted concerning visible identification card policy?		
Do employees tailgate (also called “piggybacking,” where one vehicle is directly behind another), or allow tailgating to occur as they enter or exit the facility?		
Are sign in and out logs kept at the building entrance? (If answer is no, recommend log pads be ordered in the notes section below.)		
Are sign in and out logs sufficient in stock?		
Are employees signing the log during other than normal business hours?		
Is every nonemployee without a contractor identification card signing the in and out log 24 hours a day, every day, regardless of how many times they go in and out of the facility?		
Are completed sign in and out log entries correct and legible?		
Are signs posted enforcing sign in and out policy?		
Is the security force officer(s) appearance and conduct acceptable?		
Is the security force officer(s) in a complete uniform?		
Is the security force officer(s) covering assigned post as scheduled?		
Does the security force officer(s) sign on and off duty?		
Does the security force officer(s) effectively check identification cards at building entrance(s)?		
Are sign in and out logs administered properly by the security force officer?		
Are security force officers positioned properly to observe people leaving the building?		

Question: Policies and Procedures	Yes ✓	No ✓
Is the security force officer(s) supervised and does the contract security force manager periodically check on their officers' performance?		
Are logs of supervisor visits maintained locally?		
Are significant incidents reported and documented as they occur?		
Are motor vehicle activity logs maintained and up to date, where appropriate?		
Are employee, nonemployee, and visitor logs complete and legible?		
Does the security force officer obtain employee authorization when issuing visitor passes?		
Are visitors properly escorted?		
Is package control procedure enforced?		
Are visitor passes and property passes sufficient in stock?		
Are post orders available and current? Specify date revised in notes section below.		
Are security force officer(s) provided with a current list of telephone numbers to use in an emergency?		
Are security patrols recorded and administered routinely?		
Was security force officer(s) provided on-the-job training prior to post assignment?		
Does security force officer(s) know his or her role in an emergency evacuation?		
Does the security officer participate in drills and exercises regularly to ensure compliance with policies and procedures?		
Is there a policy for effectively cutting off access to electronic information and computer systems when an employee leaves the agency?		
Are staff provided with information and training about computer security?		
Is access to all electronic information and computer systems password protected?		
Are computer passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
Is there a process for creating retrievable backup and archival copies of critical electronic information?		
Is your computing area and equipment physically secure?		

Question: Policies and Procedures	Yes ✓	No ✓
Are there procedures in place to prevent computers from being left in a logged-on state, however briefly?		
Are there procedures for protecting data during equipment repairs?		
Is security force officer(s) required to undergo a background investigation?		
What are the security force assigned posts for this facility? (attach as an appendix if applicable)		
What is the name of security force provider?		
Notes (describe deficiencies observed):		

Security Inspection Validation Technology Checklist: Card Access and Alarm

Question: Card Access and Alarm	Yes ✓	No ✓
Does the alarm system offer protection-in-depth (multiple layers of protective measures)?		
Are there any tamper protection devices hardware or lines?		
Can the alarm system perform a self-test?		
Was the alarm system properly installed?		
Does the alarm system have a high probability of detection against the threat?		
Are the false and nuisance alarm rates within acceptable standards?		
Is card access used in this building?		
Is it a networked or stand-alone system? (A networked system involves more than one facility, while a stand-alone system is for a specific site.) If the card access system is networked, write the location of the control point in the notes section below.		
Are the controls for the card access system located in a secure location?		
Can the facility provide uninterrupted power to the video assessment center?		
Are all card readers at the proper location to monitor entry?		
Are monitored contacts installed at each card reader door?		
Is a request-to-exit motion detector installed at each card reader door?		
Is a request-to-exit pushbutton installed at each card reader door using maglocks (magnetic switches used to keep doors from being opened)?		
Are all access control readers working properly?		
Are monitored contacts installed at all perimeter doors, roof hatches, and other openings?		
Are access controlled doors also equipped with an alternate means of entry, such as keys and cipher locks?		
Is there a key control program in place (a program to maintain the key inventory, who has what keys when)?		
Does the security control center operator recognize an alarm and evaluate the appropriate response?		

Question: Card Access and Alarm	Yes ✓	No ✓
What type or manufacturer is being used for the card access system?		
What is the minimum time to assess an alarm?		
What type of uninterrupted power is available (building inverter, separate uninterrupted power supply)?		
Notes (describe deficiencies observed):		

Security Inspection Validation Technology Checklist: Closed-Circuit Television

Question: Closed-Circuit Television	Yes ✓	No ✓
Are live camera images satisfactory?		
Are recorded camera images satisfactory?		
Are cameras programmed to record on event, or are they always recording?		
Are 10 seconds pre- and post-event being recorded?		
Does the recorder have alarm priority sequencing?		
Can the facility provide uninterrupted power to the security control center?		
What type of uninterrupted power is available, such as building inverter, or separate uninterrupted power supply?		
Is the power supply able to maintain security lighting and closed-circuit television coverage for critical system elements?		
Does the security control center operator recognize an alarm and evaluate the appropriate response?		
Are exterior cameras satisfactorily located to view parking areas?		
Are exterior cameras satisfactorily located to site entry and exit points (gates)?		
Are exterior cameras satisfactorily located to view building perimeter doors?		
Are interior cameras satisfactorily located to view building entry points?		
Are cameras mounted high enough to avoid tampering?		
Is camera wiring exposed to tampering?		
Which recorder manufacturer and model is being used?		
What is the coverage of the video assessment; include appropriate lighting, and zone depth and width?		

Question: Closed-Circuit Television	Yes ✓	No ✓
What type of recorder is installed (videocassette recorder, digital video recorder)?		
How many frames per second are being recorded?		
What is the resolution?		
How much video storage is available on the recorder?		
Notes (describe deficiencies observed):		

Security Inspection Validation Delaying Access Checklist: Perimeter Barriers

Question: Perimeter Barriers	Yes ✓	No ✓
Is the height of the fence material at least 2.13 meters?		
Are the spaces in the fence material less than 5 square centimeters?		
Is a top guard installed with outriggers present and three strands of barbed wire 1.8 meters apart?		
Is top guard angled out toward property exterior?		
Is razor wire installed?		
Are there any spaces between gates that could make adversaries' access easier?		
Does the fence material securely touch the ground or are there gaps?		
Is the gate susceptible to ramming?		
What type of locking devices exists at the gates?		
Could an adversary gain speed as they approached the gate or are multiple turns required to approach the gate or front of the building?		
Could the vehicle barrier defeat the threat it was designed for?		
Does detection before delay exist?		
Are gates locked when unattended?		
Are NO TRESPASSING signs posted?		
Is the security fence intact, taut, and in good repair?		
Is the area around the security fence free of any growth or object(s) within at least 1.8 meters that would enable an unauthorized person to gain entry?		
Is the security fence and gate free of openings more than 15 centimeters in diameter?		
Is the height of the gate the same as the fence?		
Does the security fence and gate reach within 5 centimeters of the ground or paving?		
Are nuts and bolts on the security fence rendered immovable?		
Are the barbed wire supports not more than 1.8 meters apart?		
Is the barbed/razor/concertina wire intact, taut and in good repair?		
If a double door gate is in use, is the vertical drop pin engaged and secured?		
Is the facility gate(s) locked or monitored when not in use?		
Are unused gates properly secured? Describe method below in notes.		

Question: Perimeter Barriers	Yes ✓	No ✓
Is there a 1.8 meter cleared area between the fence and the stored material, vehicles, tools?		
Are locks and strike plates in good working condition?		
Do doors close and latch fully?		
Are doors being propped open?		
Are automatic closing devices operating properly?		
Are all sensitive area doors locked?		
Are sensitive area doors adequately secured to prevent forced entry?		
Are sensitive area doors equipped with astragal plates (seals around the doors that prevent someone from slipping anything under, for example, to try to unlock the door) at the bottom of the doors where required?		
Have pushbutton lock combinations been changed from factory code?		
Are doors and walls free of written lock codes (notes to remind people of the codes in case they forget them)?		
If doors are alarmed, does a bell or light alert at Security Control Center or other location?		
If an alarm is triggered, is action taken?		
Is the intercom working properly?		
Can remote access be granted by way of intercom?		
If so, is visual verification available by way of video monitor?		
Are double doors locked properly?		
Are windows adequately secured to prevent forced entry?		
Are all windows accessible from the ground secured?		
Are all windows accessible from the ground alarmed? Describe method below in notes.		
Are the alarms operable?		
Are any windows that are accessible from the ground broken?		
Are air conditioning window units protected and secured?		
How frequently are pushbutton lock combinations changed?		
What type of material is the fence made of?		

Question: Perimeter Barriers	Yes ✓	No ✓
Notes (describe deficiencies observed):		

Security Inspection Validation Security Force Checklist

Question: Security Force	Yes ✓	No ✓
Does the critical infrastructure employ a security force?		
Does the security force officer(s) possess the knowledge, skills, and abilities to perform the job? (Note: you can ask the security force officer(s) job-specific questions.)		
Are mobile patrols, (foot or vehicle), carried out?		
Are there receptionists or security personnel at main reception and any other portals? <i>List hours of duty below in notes.</i>		
Do security force members respond to alarms on premise?		
What is the local law enforcement response time to the facility?		
Notes (describe deficiencies observed):		

This Page Intentionally Left Blank.