Title: Arming/Disarming Keypad Test

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Intrusion Detection System (IDS)

Notes:

1. Assumes a room with an arming/disarming keypad on the secure side, a Balanced Magnetic Switch (BMS) on the door, and motion sensor coverage.
2. Program alarm delays only for those sensors that would activate prior to the user reaching the keypad and entering the disarm code. All other sensors operate without delay.
3. Real-time voice communications between the workstation operator and the field technician is required.

Steps	Actions	Expected Results
1.0	**Arming Test**	
1.1	Ensure the room is in the ACCESS state.	Workstation indicates zone is in ACCESS state.
1.2	Input correct arming code.	No alarms are received at the workstation. Keypad and system both show SECURE.
1.3	Exit within the appropriate delay period.	No alarms are received at the workstation. Zone is SECURE.
2.0	**Disarming Test**	
2.1	Ensure the room is in the SECURE state.	Workstation indicates zone is in SECURE state.
2.2	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
2.3	Enter the correct disarming code within the delay period.	No alarms are received at the workstation. Keypad and system both show ACCESS.
2.4	Walk through the zone and attempt to activate each sensor that has been disarmed.	No alarms are received at the workstation.
2.5	Attempt to activate 24/7 alarms (such as emergency exits).	Alarm received at workstation.
2.6	Clear the alarm at the workstation.	The active alarm queue is empty.
3.0	**Incorrect Code Test - Arming**	
3.1	Ensure the room is in the ACCESS state.	Workstation indicates zone is in ACCESS state.
3.2	Input an incorrect arming code.	No alarms are received at the workstation. Keypad alerts user that system was not armed. Keypad and system both show ACCESS.
3.3	Repeat 3.2 until the maximum number of allowed attempts is reached.	Alarm received at workstation.
3.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Steps	Actions	Expected Results
4.0	**Incorrect Code Test - Disarming**	
4.1	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
4.2	Enter an incorrect disarming code.	Keypad alerts user that system did not disarm. Keypad and system both show SECURE.
4.3	Repeat 4.2 until the maximum number of allowed attempts is reached within the allotted time.	Workstation shows keypad alarm.
4.4	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Delayed Exit After Arming Test**	
5.1	Enter the correct arming code.	No alarms are received at the workstation. Keypad and workstation both show SECURE.
5.2	Exit the secure space after the programmed delay period ends.	Intrusion alarm received at the workstation after the alarm is received.
5.3	Clear the alarm at the workstation.	The active alarm queue is empty.
6.0	**Delayed Disarming Test**	
6.1	Enter the armed space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
6.2	Wait for the delay period to end.	Intrusion alarm is received at the workstation.
6.3	Enter the correct disarming code.	Keypad and workstation both show ACCESS. Alarms are still active.
6.4	Clear the alarm at the workstation.	The active alarm queue is empty.
7.0	**Duress Code Test**	
7.1	Ensure the room is in the SECURE state.	Workstation indicates zone is in SECURE state.
7.2	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
7.3	Enter the duress code within the delay period.	Alarm is received at the workstation. Keypad shows ACCESS.
7.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Title: Magnetic Lock

Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Doors and gates. Magnetic Locks. Electronic Entry Control Systems (EECS). NFPA and life safety codes.

Notes:

1. These procedures are based on interior door with card reader for entrance. This magnetic lock is installed in a fail secure configuration. On the secure side, the door has a magnetic lock with door position switch, PIR REX (Passive Infrared Request to Exit) sensor above the door, and a Push To Exit button on the wall (this is as a backup exit system).
2. All standard access control tests are needed in addition to this test. The intent of this test is to ensure egress due to the dangers of magnetic locks.
3. Ensure that the magnetic lock is installed correctly: it is flush with the closer, is on the handle side of the door, and the closer does not slam the door.
4. Assumes only one credential is required for entry (i.e. card only).
5. The Power Failure – Fail Secure Test is performed if the door is configured in "Fail Secure" mode (i.e. in a power fail situation, the door defaults to the locked condition).
6. Real-time voice communications between the workstation operator and the field technician is required.
7. For Steps 9.0 and 10.0, coordinate testing so that building occupants and emergency response forces along with all appropriate parties understand that testing is occurring.

Steps	Actions	Expected Results
1.0	**Lock Test**	
1.1	Ensure that the door is closed and locked. Contract the operator to verify that the door is secure.	Door is locked and secure.
1.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
2.0	**PIR REX Field of View Test**	
2.1	Stand slightly outside of the PIR's expected field of view	PIR does not detect test subject. Lock does not release.
2.2	Staying slightly outside of the PIR's expected field of view, walk the boundary of the PIR.	PIR does not detect test subject. Lock does not release.
3.0	**Valid Credential Test**	
3.1	Present a valid badge to the reader.	Transaction logged. Lock releases.
3.2	Open door and enter.	Door indicates as open. No alarm is received at workstation.
3.3	Close the door.	Door indicates as closed. No alarm is received at workstation. Lock reactivates when door is closed. The active alarm queue is empty.
4.0	**Invalid Credential Test**	
4.1	Present Invalid Badge to the reader.	An invalid credential alarm is received at the

Steps	Actions	Expected Results
		workstation. Transaction logged. Door lock does not release.
4.2	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Exit Test**	
5.1	Walk up to the door.	PIR releases the magnetic lock.
5.2	Walk through the door.	Door indicates as open at the workstation. Alarm does not activate.
5.3	Close the door.	Door indicates as closed. No alarm is received at workstation. Lock reactivates when door is closed. The active alarm queue is empty.
6.0	**Push-To-Exit Test**	
6.1	Walk up to the door and stand to the side (with hand on the Push To Exit button) until the PIR no longer detects the person trying to exit.	PIR releases the magnetic lock and relocks it after appropriate time. No alarm received.
6.2	Push the Push To Exit button.	Magnetic Lock releases. No alarm received.
6.3	Have person outside the room open the door.	Door opens and indicates as open at the workstation. Alarm is received at workstation.
6.4	Close the door and clear the alarm queue.	Door indicates as closed. Lock reactivates when door is closed. The active alarm queue is empty.
7.0	**Power Failure – Fail Secure Test** (This procedure is for use when lock is configured in the Fail Secure mode. I.e. lock remains active when power fails.)	
7.1	Disconnect AC power from the door controller.	
7.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
7.3	Attempt to exit through the door by means of the PIR REX.	Free egress is achieved.
7.4	Attempt to exit through the door by means of the Push To Exit button. (Stand still on the secure side of the door until the PIR disengages to do this).	Free egress is achieved.
8.0	**Power Failure – Fail Safe Test** (This procedure is for use when lock is configured in the Fail Safe mode. I.e. lock disengages when power fails.)	
8.1	Disconnect AC power from the door controller.	
8.2	Activate the door hardware from the public side and	Door opens. Door forced alarm received at the

Steps	Actions	Expected Results
	attempt open the door.	workstation.
8.3	Attempt to exit through the door from the secure side.	Free egress is achieved.
9.0	**Fire Alarm – Fail Secure Test** (This procedure is for use when lock is tied into the fire alarm system and is configured in the Fail Secure mode. I.e. lock remains active when power fails.)	
9.1	Activate the fire alarm system.	
9.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
9.3	Attempt to exit through the door by means of the PIR REX.	Free egress is achieved.
9.4	Attempt to exit through the door by means of the Push To Exit button. (Stand still on the secure side of the door until the PIR disengages to do this).	Free egress is achieved.
10.0	**Power Failure – Fail Safe Test** (This procedure is for use when lock is tied into the fire alarm system and is configured in the Fail Safe mode. I.e. lock disengages when power fails.)	
10.1	Activate the fire alarm system.	
10.2	Activate the door hardware from the public side and attempt open the door.	Door opens. Door forced alarm received at the workstation.
10.3	Attempt to exit through the door from the secure side.	Free egress is achieved.

Title: Mechanical Turnstile

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the Access Control System (ACS), and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Access control systems. Examples: Perimeter gates, fence lines, remote sites.

Notes:

1. These procedures assume a single-rotor mechanical turnstile with an entry card reader. Exit lane is the same as entry lane, and occupants are allowed free egress.
2. Assumes a single credential required for entry (i.e. card only).
3. Perform valid and invalid credential tests for entry.
4. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
5. For Valid Credential Tests (Step 2.0), use cards 1 and 2.
6. For Invalid Credential Tests (Step 3.0), use cards 3, 4, 5, and 6.
7. Real-time voice communications between the workstation operator and the field technician is required.
8. Perform these tests with the associated zone in the SECURE state.
9. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Mechanical Test**	
1.1	From the unsecure side, verify that the turnstile rotor assembly is locked. Attempt to enter from the unsecure side without a credential.	Turnstile does not allow access. No alarm received at the workstation.
2.0	**Valid Credential Access Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
2.1	Present a valid credential to the reader.	Transaction logged at workstation. Turnstile mechanical lock releases and allows rotor assembly to turn.
2.2	Pass through the turnstile.	Turnstile rotor assembly rotates to allow one person to pass through the turnstile and reactivates the mechanical lock.
3.0	**Invalid Credential Access Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
3.1	Present invalid credential to the reader.	An invalid credential alarm is received at the workstation. Turnstile does not release.
3.2	Clear the alarm at the workstation.	The active alarm queue is empty.
3.3	Repeat for each of the invalid credentials.	

Steps	Actions	Expected Results
4.0	**Egress Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
4.1	Verify turnstile rotor assembly is locked from the unsecure side.	Turnstile does not allow access. No alarm received at the workstation.
4.2	From the secure side, attempt to egress through the turnstile to the unsecure side.	Turnstile rotates to allow free egress.
4.3	Repeat 4.1 to ensure turnstile rotor assembly lock is active after egress.	Turnstile does not allow access. No alarm received at the workstation.

Title: Single Door with an Electronic Entry Control System (EECS)

Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Electronically Controlled Access Doors. These procedures are based on the system shown in UFC 4-021-02 Figure 3-5.

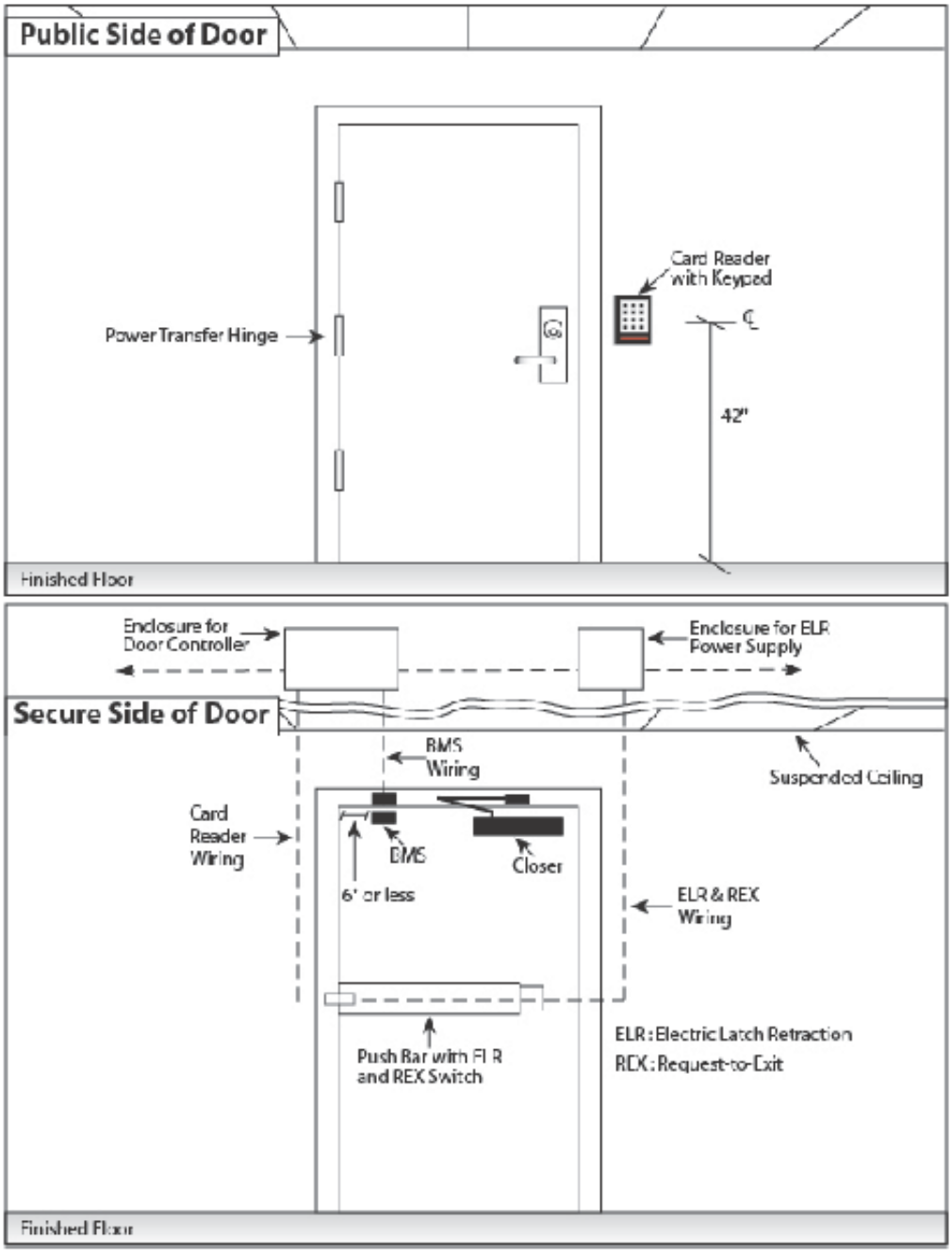
Notes:

1. These procedures are based on the system shown in UFC 4-021-02 Figure 3-5.
2. Assumes 2 credentials required for entry (i.e. card and PIN).
3. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
4. For Valid Badge Tests (Steps 3.0-5.0), use cards 1 and 2.
5. For Invalid Badge Tests (Step 6.0), use cards 3, 4, 5, and 6.
6. Real-time voice communications between the workstation operator and the field technician is required.
7. Perform these tests with the associated zone in the SECURE state.
8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.
9. Perform the tamper test on all tampers associated with the ACS portal. For example: tampers included in card readers, BMSs, door hardware, and junction boxes.

Steps	Actions	Expected Results
1.0	**Nuisance Test**	
1.1	Ensure that the door is closed and locked. Contract the operator to verify that the door is secure.	Door is locked and secure.
1.2	Without activating the door hardware, push and pull on the door to attempt to trigger a nuisance alarm.	Door does not open. No alarm received at the workstation.
2.0	**Mechanical Lock Test**	
2.1	Turn the handle and attempt to open the door.	Door does not open. No alarm received at the workstation.
3.0	**Door Forced Test**	
3.1	Either use a manual key override or open the door and fix the latch in the retracted position in such a way that the request to exit switch is not activated. Close the door. Ensure the door is shown as closed at the workstation and that the active alarm queue is empty.	Door closed. Latch retracted. The active alarm queue is empty.
3.2	Slowly open the door until the operator notifies of a door forced alarm.	Door forced alarm received at workstation before door has moved ¼ inch.
3.3	Return the door and all components to normal operating condition and ensure the door is closed.	

Steps	Actions	Expected Results
3.4	Clear the alarm at the workstation.	The active alarm queue is empty.
4.0	**Valid Badge and no PIN Test**	
4.1	Present a valid badge to the reader without entering a PIN.	Transaction logged at the workstation. Door lock does not release.
5.0	**Valid Badge and Correct PIN Test (See note 4)**	
5.1	Present a valid badge to the reader and enter the correct PIN.	Transaction logged at the workstation. Door lock releases.
5.2	Open door and enter.	Door indicates as open. No alarm is received at the workstation.
5.3	Close the door.	Door indicates as closed. Door lock reactivates. No alarm is received at workstation. The active alarm queue is empty.
6.0	**Valid Badge and incorrect PIN Test (See note 4)**	
6.1	Present a valid badge to the reader, and enter an incorrect PIN.	An invalid credential alarm is received at the workstation. Transaction logged. Door lock does not release.
6.2	Clear the alarm at the workstation.	The active alarm queue is empty.
7.0	**Invalid Badge and Correct PIN Test (See note 5)**	
7.1	Present Invalid Badge to the reader, and enter a valid PIN.	An invalid credential alarm is received at the workstation. Transaction logged. Door lock does not release.
7.2	Clear the alarm at the workstation.	The active alarm queue is empty.
8.0	**Egress Test**	
8.1	From the secure side of the door, use the push bar to egress.	Request to exit is activated. Door lock releases. Door opens. Door indicates as open at the workstation, but does not alarm.
8.2	Close the door.	Door indicates as closed at the workstation.
9.0	**Door Held Open Test**	
9.1	Open the door.	
9.2	Hold door open until the operator notifies of a door held alarm.	Door held alarm received at workstation within specified time.
9.3	Close the door.	Door indicates as closed at the workstation. Alarm is still active.
9.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Figure 3-5. Sample Card Reader Door Configuration.



Title: Vehicle Gate

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the Access Control System (ACS), and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Gates and site access. Access control systems.

Notes:

1. These procedures are based on a system consisting of a sliding vehicle gate with entry reader, safety sensor loop, and exit sensor loop.
2. Assumes a single credential required for entry (i.e. card only).
3. Perform valid and invalid credential tests for entry.
4. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
5. For Valid Credential Tests (Step 1.0), use cards 1 and 2.
6. For Invalid Credential Tests (Step 2.0), use cards 3, 4, 5, and 6.
7. Real-time voice communications between the workstation operator and the field technician is required.
8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.
9. Perform these tests with the associated zone in the SECURE state.

Steps	Actions	Expected Results
1.0	**Valid Credential Access Test**	
1.1	Approach gate with vehicle from the unsecure side.	Gate does not open. No alarm received.
1.2	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
1.3	Drive through the gate.	After appropriate hold time, gate closes while sounding local area buzzer.
2.0	**Invalid Credential Access Test** (see note 3)	
2.1	Present Invalid credential to the reader.	An invalid credential alarm is received at the workstation. Gate does not open.
2.2	Clear the alarm at the workstation.	The active alarm queue is empty.
3.0	**Safety Loop Test**	
3.1	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
3.2	Place a metal plate on the safety loop.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
3.3	Remove the metal plate and clear the alarm at the workstation.	Gate closes while sounding local area buzzer. The active alarm queue is empty.

Steps	Actions	Expected Results
3.4	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
3.5	Drive into the gate path and stop.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
3.6	Move vehicle away from gate.	Gate does closes while sounding local area buzzer. Blocked gate alarm still active at workstation.
3.7	Clear the alarm at the workstation.	The active alarm queue is empty.
4.0	**Vehicle Block Test**	
4.1	Present a valid credential to the reader.	Transaction logged. Gate opens.
4.2	Stand Near the gate path, being careful not to block the path of the gate.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
4.3	Walk away from gate.	Gate does closes while sounding local area buzzer. Blocked gate alarm still active at workstation.
4.4	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Exit Test**	
5.1	Drive vehicle to gate from the inside.	Gate opens while sounding local area buzzer. No alarm received.
5.2	Drive through the gate.	After appropriate hold time, gate closes while sounding local area buzzer.

Title: Image Quality (Day and Night)

Objective: Verify system is installed using acceptable standards and practices, communicates properly, and meets or exceeds the contract performance specification.

Applicability: Closed Circuit Television (CCTV) System, Video Management Software (VMS)

Notes:

1. If this test is performed on a camera system displaying multiple cameras on the same monitor, then view the video from each camera in full screen mode.
2. Perform all tests on every camera.
3. For pan, tilt, zoom cameras, perform these tests using the default/home positions.
4. In some cases, if acceptable to end user and contract documents, it is appropriate to conduct these tests based on recorded video.
5. In locations where specific weather patterns (such as frequent rain) typically occur, consider performing the same steps from the day/night testing for that weather condition.
6. Nighttime test can be done in either pre-dawn or post-sunset, preferably not during a full moon in order to better test worst-case conditions.
7. Verify that security lighting is operating according to the site's standard operating procedures.
8. Real-time voice communications between the workstation operator and the field technician are required.

Steps	Actions	Expected Results
1.0	**Daytime Video Quality Test**	
1.1	If applicable direct a test subject (person or vehicle) to enter the field of view.	
1.2	Once image is brought to full screen, verify the following:	The video image is clear. Test subject's movement in the video image is smooth, not choppy.
1.3	The video image is in focus.	The video image is sharp, clear and distinct.
1.4	The video image is stable.	The video image does not move or sway.
1.5	The video image has sufficient resolution and quality.	The video image meets the contract performance specifications and is without pixilation, rolling, flickering, discoloration, and glare from light sources.
2.0	**Nighttime Video Quality Test**	
2.1	If applicable direct a test subject (person or vehicle) to enter the field of view.	
2.2	Once image is brought to full screen, verify the following:	The video image is clear. Test subject's movement in the video image is smooth, not choppy. If applicable, the camera has shifted to the correct day/night mode.
2.3	The video image is in focus.	The video image is sharp, clear and distinct.
2.4	The video image is stable.	The video image does not move or sway.

Steps	Actions	Expected Results
2.5	The video image has sufficient resolution and quality.	The video image meets the contract performance specifications and is without pixilation, rolling, flickering, discoloration, and glare from light sources.
3.0	**Video Specifications Validation Test**	
3.1	Open the camera options menu and verify the following settings are set in accordance with the contract requirements:	
3.2	Frame Rate	The camera is recording at the specified frame rate. The frame rate is sufficient for the video to meet its intent.
3.3	Recording Resolution	The camera is being recorded at the resolution required by the contract.
4.0	**Field of View Test**	
4.1	Verify that the camera field of view meets the intent of the camera and satisfies the contract requirements.	Required areas are covered. Video does not show significant dead space (for example: ceilings).
5.0	**Video Loss Detection Test**	
5.1	Disconnect the camera from the video storage device.	The video image goes blank, and the video lost message appears.
5.2	Reconnect the camera to the video storage device.	The video image returns, and the video lost message is no longer present.

Title: Active Infrared Sensor
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Active Infrared Sensors, Photoelectric Sensors. Example: Covering doors, windows and other openings.
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the sensor tamper test. 3. Perform the intrusion test with the associated zone in the SECURE state. 4. Enable sensor motion test lights for conducting these tests. Deactivate after testing is completed. 5. Line Supervision, Power Fail, and Tamper Tests (tamper test each cover on the beam tower/array) need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Stand outside of the detection beams and ensure that the detection path is clear.	No alarms are received at the workstation.
1.2	Attempt to pass through the detection area.	An intrusion alarm is received at the workstation.
1.3	Stand clear of the detection area.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
2.0	**Beam Test**	
2.1	Block only one beam on the sensor tower/array.	An intrusion alarm is received at the workstation.
2.2	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
2.3	Repeat for each individual beam on the sensor tower/array.	

Title: Balanced Magnetic Switch (BMS)
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the workstation, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Examples: Doors, gates, hatches, and operable windows.
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the BMS tamper tests. 3. Perform the nuisance test and intrusion test with the associated zone in the SECURE state. 4. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Nuisance Test**	
1.1	Rattle or shake the door to simulate normal vibrations that might be induced by wind or other non-intrusion factors.	No alarm is received at the workstation.
2.0	**Intrusion Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
2.1	Gradually open the door until an alarm occurs. (This assumes that the door alarm is not programmed with an entry delay.)	An intrusion alarm is received at the workstation when greater than ¼ inch movement of the magnet in relation to the switch housing.
2.2	Close the door.	
2.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.

Title: Beam Break Sensor
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Active Infrared Sensors, Photoelectric Sensors.
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. Make penetration attempts using methods and locations that minimize the chance of detection. 3. The field technician may need tools and a stepladder to perform the sensor tamper test. 4. Perform the intrusion test with the associated zone in the SECURE state. 5. Enable sensor motion test lights for conducting these tests. Deactivate after testing is completed. 6. Line Supervision, Power Fail, and Tamper Tests (tamper test each cover on the beam tower/array) need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test – Beam Cross**	
1.1	Stand outside of the detection beams and ensure that the detection path is clear.	No alarms are received at the workstation.
1.2	Attempt to pass through the detection area.	An intrusion alarm is received at the workstation.
1.3	Stand clear of the sensor detection pattern.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
2.0	**Beam Test**	
2.1	Block only one beam on the sensor tower/array.	An intrusion alarm is received at the workstation.
2.2	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
2.3	Repeat for each individual beam on the sensor tower/array.	
3.0	**Intrusion Test – Post Climb**	
3.1	Stand outside of the detection beams and ensure that the detection path is clear.	No alarms are received at the workstation.
3.2	Attempt to climb the post (do not climb over the top).	An intrusion alarm is received at the workstation.
3.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.

Title: Passive Infrared Sensor – Curtain Type
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Curtain Passive Infrared Sensors
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the sensor tamper test. 3. Perform intrusion tests with a human target. All observers are to remain still and clear of the detection zone to avoid triggering the alarm and creating invalid results. 4. Prior to the start of testing, mark five intrusion lanes (or points of intrusion taking into account the sensor coverage area), with each lane probing a different portion of the sensor detection pattern. Test each intrusion lane. 5. Perform the intrusion test with the associated zone in the SECURE state. 6. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Stand at the beginning of the intrusion lane and remain motionless for 20 seconds.	No alarms are received at the workstation.
1.2	Step into intrusion lane.	An intrusion alarm is received at the workstation.
1.3	Move out of the sensor detection pattern.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.5	Repeat for all lanes (note # 4).	

Title: Dual Technology Sensor
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Dual technology sensors (microwave and passive infrared)
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the sensor tamper test. 3. Perform intrusion tests with a human target. All observers are to remain still and clear of the detection zone to avoid triggering the alarm and creating invalid results. 4. Prior to the start of testing, mark five intrusion lanes (or points of intrusion taking into account the sensor coverage area), with each lane probing a different portion of the sensor detection pattern. Test each intrusion lane. 5. Perform the intrusion with the associated zone in the SECURE state. 6. If multiple sensors are used to protect an alarmed zone, disable all sensors except the unit being tested. Restore all sensors to normal operation following the completion of testing. 7. If equipped, enabling sensor motion test light is useful for conducting these tests. Deactivate after testing is completed. 8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Stand at the beginning of the intrusion lane and remain motionless for 20 seconds or until test light turns off.	No alarms are received at the workstation.
1.2	Take four steps at a normal walking pace along the intrusion lane and stop.	An intrusion alarm is received at the workstation.
1.3	Move out of the sensor detection pattern.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.5	Repeat for all lanes (note # 4).	

Title: Fence Sensor

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the ACS, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Fiber optic sensing cable, fence mounted vibration sensors, strain sensitive cable sensors.

Notes:

1. Real-time voice communications between the workstation operator and the field technician is required.
2. The field technician will need a screwdriver, protective equipment and a stepladder to perform the fence sensor test.
3. Make penetration attempts using methods and locations that minimize the chance of detection.
4. Simulated cut test will use a screwdriver to tap on the fence fabric. Ensure the number of taps exceeds the event count calibration value.
5. Apply a similar force to that needed to cut the fence fabric for each simulated cut test tap.
6. If sensing cable is in the outrigger, the simulated Cut test needs to be performed on the outrigger also.
7. Do not climb over the fence or into the outrigger.
8. Establish number of tests and test locations per the requirements.
9. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test – Simulated Cut**	
1.1	Intruder will position themselves at the section of fence to be tested.	No alarms are received at the workstation.
1.2	Tap the screwdriver at different locations on the fence panel and vertical outrigger at approximately one-second intervals.	An intrusion alarm is received at the workstation.
1.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
2.0	**Intrusion Test – General**	
2.1	Intruder will position themselves at the section of fence to be tested.	No alarms are received at the workstation.
2.2	Grab and firmly shake the fence fabric to attempt to set off an alarm.	An intrusion alarm is received at the workstation.
2.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
3.0	**Intrusion Test – Fence Climb**	
3.1	Intruder will position themselves at the section of fence to be climbed.	No alarms are received at the workstation.
3.2	Intruder will begin to climb the fence.	An intrusion alarm is received at the workstation.
3.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
4.0	**Nuisance Test**	
4.1	Intruder will position themselves at the section of	No alarms are received at the workstation.

Steps	Actions	Expected Results
	fence to be tested.	
4.2	Grab and rattle the fence to simulate wind on the fence.	No intrusion alarms are received at the workstation.

Title: Glass Break Sensor - Acoustic Type
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Glass Break Sensors (Acoustic Type)
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician will need a Glass Breakage Tester unit (and potentially a stepladder and other tools) to perform the tests. 3. Perform all tests with the associated zone in the ACCESS state. 4. If multiple sensors are used to protect an alarmed zone, disable all sensors except the unit being tested. Restore all sensors to normal operation following the completion of testing. 5. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Position testing unit on the glass pane furthest away from the sensor but at a distance no greater than the sensors range published by the manufacturer. Activate the testing unit.	An intrusion alarm is received at the workstation. If equipped, a visual alarm (light) will be displayed. After completion of test and prior to performing additional tests, verify that the visual alarm is reset.
1.2	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.3	Repeat for each of the corners of the covered glass farthest from the center of the coverage zone.	

Title: Glass Break Sensor - Contact Type
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Glass Break Sensors (Contact Type)
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the test. 3. Conduct the intrusion test with a lightweight tool such as the plastic handle of a screwdriver. 4. Perform all tests with the associated zone in the ACCESS state. 5. If multiple sensors are used to protect an alarmed zone, disable all sensors except the unit being tested. Restore all sensors to normal operation following the completion of testing. 6. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Lightly rap the glass in the corner farthest from the sensor.	An intrusion alarm is received at the workstation.
1.2	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.

Title: Interior Volumetric Sensor
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Passive infrared, microwave, and dual technology sensors
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the sensor tamper test. 3. Perform intrusion tests with a human target. All observers are to remain still and clear of the detection zone to avoid triggering the alarm and creating invalid results. 4. Prior to the start of testing, mark five intrusion lanes (or points of intrusion taking into account the sensor coverage area), with each lane probing a different portion of the sensor detection pattern. Test each intrusion lane. 5. Perform the intrusion test with the associated zone in the SECURE state. 6. If multiple sensors are used to protect an alarmed zone, disable all sensors except the unit being tested. Restore all sensors to normal operation following the completion of testing. 7. If equipped, enabling sensor motion test light is useful for conducting these tests. Deactivate after testing is completed. 8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Stand at the beginning of the intrusion lane and remain motionless for 20 seconds or until test light turns off.	No alarms are received at the workstation.
1.2	Take four steps at a normal walking pace along the intrusion lane and stop.	An intrusion alarm is received at the workstation.
1.3	Move out of the sensor detection pattern.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.5	Repeat for all lanes (note # 4).	

Title: Microwave Sensors
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Bi-static microwave and mono-static microwave
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. Make penetration attempts using methods and locations that minimize the chance of detection. 3. It is acceptable to use calibrated substitutes for a human intruder. For example, a 12-inch (30 cm) diameter aluminum sphere pulled at grade across the detection zone may be permissible. 4. Instruct all observers to stand away from the coverage zone in order to avoid triggering an alarm and creating invalid results. 5. Perform the walk test at a normal pace. Allow practice runs for the run-and-jump test in order to approximate the location of the zone to better time the jump to clear the zone. Conduct the crawl test at a slow, steadily paced crawl. If applicable at a vehicle gate, perform the intrusion test using a vehicle. Vary test speed in the range of 0.2 to 25 feet/second. 6. Perform intrusion tests approximately every 10 feet or less depending on the zone length. 7. Perform the Intrusion Tests with the associated zone in the SECURE state. 8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures. 9. Perform the tamper test on all transmitters, receivers, and field distribution boxes. 10. If equipped, enabling sensor motion test lights or tones is useful for conducting these tests. Deactivate after testing is completed.

Steps	Actions	Expected Results
1.0	**Intrusion Test – Walking, Run-and-Jump, Crawling, Vehicle**	
1.1	Stand outside of the coverage zone.	No alarms are received at the workstation.
1.2	Cross the coverage zone.	An intrusion alarm is received at the workstation.
1.3	Stop outside of the coverage zone.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.5	Repeat for each entry method along the coverage zone.	

Title: Buried Ported Coax Sensors

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Perimeters

Notes:

1. Real-time voice communications between the workstation operator and the field technician is required.
2. The sensor may be equipped with an integral test indicator. If present, verify that the test indicator is operable and visible during the test.
3. Instruct all observers to stand away from the coverage zone in order to avoid triggering the alarm and creating invalid results.
4. Make penetration attempts using methods and locations that minimize the chance of detection. Areas of note are beginning and ending of cable runs, crossovers, transitions to different ground medium, areas after sharp bends in the cable paths, and locations in close proximity to fencing and other metal objects.
5. Make intrusion attempts across the sensor cable at approximately 10-foot intervals. Adjust this interval at the termination points of the two sensor cable pairs.
6. Vary test speed in the range of 0.2 to 25 feet/second.
7. Allow practice runs for the run-and-jump test to approximate the location of the zone to better time the jump to clear the zone.
8. Perform the intrusion tests with the associated zone in the SECURE state.
9. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test – Walking and Run-and-Jump**	
1.1	Stand outside of the coverage zone.	No alarms are received at the workstation.
1.2	Cross the coverage zone.	An intrusion alarm is received at the workstation.
1.3	Stop outside of the coverage zone.	
1.4	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.5	Repeat for each testing method.	
2.0	**Remote Test**	
2.1	Verify that there are no active alarms along the sensor path.	
2.2	Activate the remote test.	Alarm received at the workstation.
2.3	Clear the alarm at the workstation.	The active alarm queue is empty.

Title: Taut Wire Sensor
Objective: Verify device is installed using acceptable standards and practices, communicates properly with the IDS, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Fences, perimeters.
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools, protective equipment, and a stepladder to perform the sensor tamper test. 3. When conducting the deflection test, do not pull wires beyond a 2 inch deflection. This is to avoid damaging the system. 4. Make penetration attempts using methods and locations that minimize the chance of detection. 5. Conduct tests for each wire at the point farthest from the sensor posts. 6. Conduct the tamper test for field distribution boxes, sensor posts, and sensor post junction boxes (if used).

Steps	Actions	Expected Results
1.0	**Intrusion Test – Deflection Test**	
1.1	Attach a measurement tool (like a yardstick) behind the wire to be tested.	No alarms are received at the workstation.
1.2	Slowly pull the wire down and measure the vertical deflection required to trigger an alarm. (See note 3.)	An intrusion alarm is received at the workstation.
1.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.
1.4	Repeat for each wire.	

Title: Vibration Sensor
Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Vibration Sensors. Example: covering vaults and arms rooms.
Notes: 1. Real-time voice communications between the workstation operator and the field technician is required. 2. The field technician may need tools and a stepladder to perform the sensor tamper test. 3. Take care so as not to damage any surfaces while conducting this test. 4. Test may require multiple impacts to trigger sensor depending on the sensor configuration. 5. Perform the intrusion tests with the associated zone in the SECURE state. 6. If multiple sensors are used to protect an alarmed zone, disable all sensors except the unit being tested. Restore all sensors to normal operation following the completion of testing. 7. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Intrusion Test**	
1.1	Stand still near the sensor.	No alarms are received at the workstation.
1.2	Create a vibration. Example: strike the wall with a rubber mallet at different locations within the manufacturer's rated coverage area.	An intrusion alarm is received at the workstation.
1.3	Clear the intrusion alarm at the workstation.	The active alarm queue is empty.

Title: Line Supervision Test
Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification. Also verifies the ability of a system to recover after a communications failure.
Applicability: Sensors, Transmission lines, Panels (FDBs and ACUs), Workstations, Servers, IDS, ACS.
Notes: 1. Procedures are designed assuming a system consisting of an Access Control Unit (ACU) (for example a door controller) with associated devices that is connected to a workstation. 2. The field technician may need keys to access components in locked rooms for these tests. 3. A detailed link testing list is essential to ensuring 100% system testing. 4. The purpose of alarm annunciation is to provide a correct and useful location of the alarm. 5. Real-time voice communications between the workstation operator and the field technician is required. 6. Verify that alarms annunciate quickly and meet appropriate standards.

Steps	Actions	Expected Results
1.0	**Communications Failure and Access Control Unit (ACU) Test**	
1.1	Disconnect the network communication line at the ACU.	Network communication failure alarm received at the workstation.
1.2	Repeat access, access denied, egress, and alarm (door held or door forced) tests.	Tests results are consistent with the results from the respective tests, but alarms are not received at the workstation.
1.3	Reconnect the communications line.	Workstation receives all system transaction logs and alarms from tests performed while communications were disconnected. Workstation shows communications have been restored.
1.4	Clear the alarms at the workstation.	The active alarm queue is empty.
2.0	**ACU to Credential Verification Device Failure Test**	
2.1	Disconnect the communication line from the ACU to the credential verification device.	Line supervision alarm received at the workstation.
2.2	Repeat Valid Credential test.	Device is unresponsive, door lock does not release.
2.3	Reconnect the communication line from the ACU to the credential verification device.	Line supervision alarm is still active.
2.4	Clear the alarms at the workstation.	The active alarm queue is empty.
2.5	Repeat Valid Credential test.	Transaction logged at the workstation. Door lock releases.
3.0	**Open Circuit Test (conduct this test for each**	

Steps	Actions	Expected Results
	device)	
3.1	Disconnect the device signal lead from the ACU.	Line supervision alarm received at the workstation.
3.2	Reconnect the device signal lead from the ACU.	The alarm is still active.
3.3	Clear the alarms at the workstation.	The active alarm queue is empty.
4.0	**Short Circuit Test (conduct this test for each device)**	
4.1	Place a jumper wire across the terminal blocks for the input and short the device's input wires together.	Line supervision alarm received at the workstation.
4.2	Remove the jumper wire.	The alarm is still active.
4.3	Clear the alarms at the workstation.	The active alarm queue is empty.

Title: Power Failure Test
Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Backup Power, ACS, IDS
Notes: 1. Procedures are designed assuming a system consisting of an Access Control Unit (ACU) (for example a door controller) with associated devices that is connected to a workstation. 2. Take appropriate safety precautions because this test involves energized power sources. 3. If backup power is batteries, a multi-meter or voltage meter is required to test voltage. 4. Real-time voice communications between the workstation operator and the field technician is required. 5. Perform these tests with the associated zone in the SECURE state.

Steps	Actions	Expected Results
1.0	**AC Power Loss and Restoration Test**	
1.1	Disconnect AC power from the ACU.	AC power failure alarm is received at the workstation. No intrusion alarms are generated from the power loss. System continues to operate correctly.
1.2	Reconnect AC power to the ACU.	Workstation notifies that AC power has been restored. No intrusion alarms are generated from the change in power source. System continues to operate correctly. AC power failure alarm is not cleared until acknowledged at the workstation.
1.3	Clear alarm at workstation.	Active alarm queue is empty.
2.0	**Backup Power Duration Test**	
2.1	Allow the system to run under normal conditions on battery power. Note the time of disconnection from AC power. (If backup power is a battery, measure the voltage of the battery immediately after disconnecting AC power).	System switches to backup power without issues. (If battery backup is used, document the measured voltage.)
2.2	Allow the system to run until at least the required duration has passed. (If backup battery is used, measure the voltage of the battery prior to reconnecting the AC power in the next step).	System operated correctly for the entire required duration. (If battery backup is used, document the measured voltage.)
2.3	Reconnect AC power.	System switches to AC power without issues.
3.0	**Battery Recharge Test (if applicable)**	
3.1	After Backup Power Duration Test has been performed, reconnect AC power and note the time.	System switches to AC power without issues.
3.2	Allow the system to run for the required recharge duration.	System operated correctly for the entire required duration.
3.3	Measure the battery's voltage.	Voltage on the battery has returned to full value as measured in the Backup Power Duration Test.

Title: Tamper Test
Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.
Applicability: Almost all devices and equipment covers; all panels.
Notes: 1. Perform the tamper tests with the associated zone in the ACCESS state. 2. Perform the tamper test on all tampers associated with every device in the system. For example: tampers included in card readers, BMSs, door hardware, and junction boxes. 3. The Tamper Switch Test is for tampers inside the component. 4. The Mounting Tamper Test is for tampers that go between the device and the mounting surface. This test is to be performed if applicable.

Steps	Actions	Expected Results
1.0	**Tamper Switch Test**	
1.1	Gradually remove the cover of the device, junction box, or panel until an alarm occurs.	A tamper alarm is received at the workstation before the tamper switch is accessible and before there is direct line of sight to any internal components.
1.2	Reattach the cover.	
1.3	Clear the tamper alarm at the workstation.	The active alarm queue is empty.
2.0	**Mounting Tamper Test (if applicable)**	
2.1	Attempt to non-destructively remove the device from the mounting surface.	Alarm received at workstation before any components or wiring are visible.
2.2	Reattach the cover.	
2.3	Clear the tamper alarm at the workstation.	The active alarm queue is empty.

Functional Test Log

Project:

Procedure:

Device ID	Location	Enter Date and Pass/Fail Result for Each Attempt		

Failure Explanation

Device ID	Cause	Corrective Action

NOTES:

Burn-In Test Log
Project:
Test Start Date & Time: **Test End Date & Time:**

Date	Time	Component / Feature	Description of Anomaly	Corrective Action	Repeated Functional Tests

NOTES: