

New construction security integration: a timeline guide for Colorado general contractors

A practical reference for GCs managing commercial new construction or tenant improvement projects in Colorado. Use this timeline to coordinate security system rough-in, installation, and commissioning with your overall project schedule. Security touches multiple trades, and when it is treated as an afterthought, the result is rework, surface-mounted cabling, and avoidable change orders.

PHASE 1 Pre-construction

8 to 12 weeks before groundbreaking

Scope the security system during design, not after permits are pulled. Decisions made here affect every later phase.

- **Select the security integrator and finalize the system design.** The integrator needs architectural drawings to plan conduit routes, door hardware, camera placements, and panel locations.
- **Confirm specified platforms and authorization.** Verify the integrator holds manufacturer authorization for the specified platforms (Genetec, Gallagher, Axis, and others). This affects warranty coverage, software licensing, and long-term support.
- **Identify all access-controlled door locations.** The integrator needs this before the door schedule is finalized, because electric strikes, mag locks, and request-to-exit devices each require different frame prep and power.
- **Establish conduit pathways.** Plan low-voltage runs from the server/head-end room to every camera location, door, alarm panel, and intercom.
- **Coordinate electrical scope.** Confirm dedicated circuits for the head-end room, any PoE switches, and fire alarm panels with the electrical contractor.
- **Flag CJIS scope if applicable.** If the project requires CJIS compliance (law enforcement, courts, corrections), confirm it during design. CJIS drives decisions about network segmentation, encryption, and physical server placement that are difficult to retrofit.

PHASE 2**Rough-in**

Concurrent with electrical and framing

The most coordination-intensive phase for security integration. Anything missed here gets expensive later.

- **Pull low-voltage cabling before walls close.** Cat6 or Cat6A to every camera location, access control door, intercom, and alarm panel. Retrofitting cabling after drywall is installed costs 3 to 5 times more than getting it right during rough-in.
- **Install conduit for sensitive runs.** Required for any cable crossing fire-rated walls, exterior walls, or areas with high electromagnetic interference (near electrical panels, HVAC equipment, elevators).
- **Coordinate door frame prep.** The door hardware vendor, frame manufacturer, and security integrator all need to align. A frame prepped for a standard lock but not for an electric strike will need to be replaced or modified on site.
- **Mount back boxes at correct heights.** Intercom stations, alarm keypads, and card readers all have ADA mounting requirements (card readers at 48 inches maximum to the center of the device).
- **Stage the head-end room.** Install the rack or cabinet, and confirm power, cooling, and network connectivity are in place or on the electrical schedule.

PHASE 3**Post-drywall / trim**

After walls are finished, before certificate of occupancy inspection

- **Mount visible devices.** Cameras, card readers, keypads, request-to-exit sensors, and intercom stations.
- **Install door hardware.** Electric strikes, mag locks, door contacts. Test each door for proper latching, alignment, and lock/unlock function before the integrator programs the system.
- **Terminate and test all cabling.** Both at the head-end rack and at each device location. Test every cable run for continuity and performance.
- **Coordinate with IT on shared structured cabling.** When the system supports both IT and security (common on modern commercial projects), coordinate termination and labeling. Mislabelled or untested runs cause commissioning delays.

1 to 2 weeks before occupancy

The integrator programs and tests the full system, then hands it off to the facility owner.

- **Program access control.** Credential groups, schedules, access levels, lockdown protocols, and door-held/forced-door alarms.
- **Program video surveillance.** Camera views, recording schedules, motion detection zones, and remote access.
- **Program intrusion detection.** Sensor zones, arming schedules, and alarm notification routing.
- **Test every device and every scenario.** Door open/close, alarm trigger, camera recording on event, credential grant/deny, lockdown activation, and fire alarm integration (verify that fire alarm activation releases mag locks, as required by code).
- **Walk the system with the owner.** Confirm the facility manager can operate the management software, pull footage, add or revoke credentials, and generate reports.
- **Hand over as-built documentation.** System drawings, device locations, cable labeling schedules, and login credentials for all management platforms.

Fire alarm integration note

In Colorado, fire alarm systems require a separate permit and inspection from the local authority having jurisdiction (AHJ). Fire alarm commissioning typically runs on its own schedule, but the security integrator needs to coordinate two things with the fire alarm contractor:

1. **Mag lock release on fire alarm activation.** Mag locks on access-controlled doors must release when the fire alarm activates. This is a code requirement, not an option. Test this integration during commissioning.
2. **Shared monitoring pathways.** If the security system and fire alarm share a monitoring connection (common when both report to the same central station), confirm the monitoring pathways are correctly programmed and that alarm signals route to the right response protocol.

These four issues generate the most change orders and schedule delays on commercial security integration.

1. **Door frames not prepped for electrified hardware.** If the frame order goes out before the security integrator reviews the door schedule, the frames arrive without the cutouts and wiring channels the hardware requires.
2. **Low-voltage cabling omitted from the rough-in schedule.** When cabling gets treated as a separate scope and scheduled after drywall, every cable pull becomes a surface mount or a costly fish-through-finished-walls exercise.
3. **Head-end room not ready at commissioning.** The integrator cannot program or test the system if the rack, power, cooling, and network are not operational.
4. **No ADA coordination on device mounting heights.** Card readers, keypads, and intercoms all have ADA mounting height requirements. If wall blocking or conduit stubs are placed at the wrong height during rough-in, devices either violate ADA or require rework.

Quick reference: when to involve the security integrator

Project phase	Security integrator involvement
Design / pre-construction	System design, platform selection, conduit planning, door schedule review
Permitting	Fire alarm permit coordination (if applicable)
Rough-in	Low-voltage cabling, conduit, door frame prep, back box installation, head-end room prep
Post-drywall / trim	Device mounting, cable termination, hardware installation
Commissioning	System programming, full testing, facility manager walkthrough, as-built documentation
Post-occupancy	Warranty support, system training, ongoing maintenance

About ESI Technologies

ESI installs commercial security systems on new construction and tenant improvement projects across Northern Colorado (Fort Collins, Loveland, Greeley, Windsor, Longmont) and Southern Colorado (Colorado Springs, Pueblo, Monument, Castle Rock).

Manufacturer authorizations: **Genetec, Axis, Gallagher, Avigilon, AMAG, Salto**. NICET certification for fire alarm work, with CJIS-cleared technicians for law enforcement and government projects.

Call **(970) 999-1681** (Northern CO) or **(719) 602-7336** (Southern CO) to bring an integrator into design review on your next project.