

Courthouse Security Assessment Checklist

Use this checklist as a self-assessment aid to review your courthouse's security program, facility, and operations. Walk the building at different times of day, talk with the people who work there, and record conditions and owners for each finding rather than simple yes/no answers. Results can guide an internal review or help you prepare for a professional assessment.

1. Governance and Program

- ☐ A court security committee (or equivalent) exists with judicial, administrative, law enforcement, and facilities representation
- ☐ Written security policies and procedures are current and approved
- ☐ Roles are defined among the court, the sheriff or security provider, and building management
- ☐ Incident reporting is in place, and incidents are tracked and reviewed
- ☐ A security budget and a capital improvement plan exist and are prioritized
- ☐ A threat management process exists for threats against judges and staff

2. Exterior and Perimeter

- ☐ Site lighting is adequate at entrances, parking, walkways, and loading areas
- ☐ Landscaping doesn't create concealment or block sightlines
- ☐ Vehicle standoff and barriers protect public entrances and vulnerable façades
- ☐ Exterior doors are secured, alarmed, and monitored; unused doors are controlled
- ☐ Ground-floor windows and rooftop access points are evaluated
- ☐ Utilities, generators, and air intakes are protected from tampering
- ☐ Signage clearly directs the public to the screened entrance

3. Parking

- ☐ Judges and key staff have secure, separate parking
- ☐ Parking assignments don't display names or titles
- ☐ Access control and camera coverage are in place for secure parking
- ☐ Routes from parking to the building are protected and well lit

4. Public Entrance and Screening

- ☐ All public visitors pass through a single screening point (or as few as possible)
- ☐ Magnetometers and X-ray equipment are functional, maintained, and properly staffed
- ☐ Written screening procedures cover prohibited items, secondary screening, and refusals
- ☐ Screening staff are trained and their performance is periodically tested
- ☐ The queue area protects people waiting from outside threats and weather
- ☐ Policy on staff and attorney screening is defined and consistently enforced
- ☐ Duress alarms are at the screening station, and there's a response plan
- ☐ Storage or handling of prohibited items is defined

5. Circulation and Zoning

- ☐ Public, restricted (staff/judicial), and secure (in-custody) circulation paths are separated
- ☐ In-custody defendants never pass through public corridors, or exceptions are controlled and escorted
- ☐ Judges can move between chambers, courtrooms, and parking without crossing public areas
- ☐ Access control enforces zone boundaries, and credentials are managed (issued, audited, revoked)
- ☐ Keys are controlled and inventoried
- ☐ Stairwells and elevators are evaluated for zone integrity

6. Courtrooms

- ☐ Duress alarms at the bench, clerk, and other stations are tested on a schedule
- ☐ The bench design gives reasonable protection and a clear exit route for the judge
- ☐ Court security staffing levels match case type and risk
- ☐ In-custody entry to the courtroom is separate and controlled
- ☐ Courtrooms are swept before use and secured when not in use
- ☐ Procedures exist for high-risk or high-profile proceedings
- ☐ Furniture and fixtures don't provide potential weapons (loose items, glass)

7. Chambers and Staff Areas

- ☐ Chambers suites have access control and duress alarms
- ☐ Reception areas use counters, controlled doors, or other means to separate visitors from staff
- ☐ Clerk's office and public-service counters are protected, with duress capability
- ☐ Cash-handling areas follow secure procedures
- ☐ After-hours access and lone-worker procedures exist

8. Holding and In-Custody Areas

- ☐ Holding cells are secure, inspected, and monitored
- ☐ Sally port and transport procedures are documented
- ☐ Prisoner movement is escorted and recorded
- ☐ Staffing ratios for in-custody movement are adequate

9. Jurors, Witnesses, and Vulnerable Parties

- ☐ Jury assembly and deliberation rooms are in restricted areas
- ☐ Waiting areas separate victims and witnesses from defendants where possible
- ☐ Family and protective order courts have added security measures

10. Electronic Security Systems

- ☐ Camera coverage includes entrances, screening, corridors, courtrooms, holding, and parking
- ☐ Video is recorded, retained for a defined period, and monitored where needed
- ☐ The intrusion detection system covers the perimeter and sensitive rooms
- ☐ Duress alarm annunciation goes to a staffed location with a defined response
- ☐ Systems are maintained, tested, and documented
- ☐ Systems are integrated where appropriate, and the design is based on requirements rather than a single vendor's product line

11. Mail, Deliveries, and Contractors

- ☐ Mail and packages are screened before distribution
- ☐ Staff are trained to recognize suspicious items
- ☐ The loading dock is controlled and monitored
- ☐ Contractors and vendors are vetted, badged, and escorted as appropriate

12. Emergency Preparedness

- ☐ A current Occupant Emergency Plan covers evacuation, shelter in place, and lockdown
- ☐ Procedures account for in-custody persons, jurors, and the public during emergencies
- ☐ Bomb threat and suspicious package procedures are in place
- ☐ Active threat procedures have been coordinated with law enforcement
- ☐ Emergency notification works across courtrooms, chambers, and public areas
- ☐ Drills and tabletop exercises are held, and lessons learned are documented
- ☐ A continuity of operations plan exists for court functions

13. Training and Awareness

- ☐ Security staff receive initial and recurring training
- ☐ Judges and court staff receive security awareness training
- ☐ Staff know how to report threats and concerning behavior
- ☐ Workplace violence prevention training and reporting are in place

14. Information and Cybersecurity Touchpoints

- ☐ Personal information about judges and staff is protected from public disclosure where policy allows
- ☐ Security system networks are separated from public networks
- ☐ Security plans and drawings are access-controlled

Turning Findings Into Action

For each finding, record: (1) the vulnerability — what could happen, and where; (2) the risk — likelihood and consequence; (3) options — procedural, physical, or electronic measures with rough cost ranges; (4) priority and owner — who acts and by when. Start with low-cost procedural fixes while capital improvements move through budgeting, and document everything.