ACCESS CONTROL AND IDENTITY VERIFICATION

Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

MISSION AREA

Protection

FUNCTIONAL AREAS

• Controlling cyber access
• Controlling physical access
• Verifying identity

EXAMPLE WORDING

Local partners provide cyber awareness training for employees, utilize virus detection software, and restrict electronic access to computer systems, especially those controlling critical infrastructure components (i.e. SCADA) or containing sensitive data.

Utilities and other critical lifeline sites restrict physical entry to employees or escorted guests with valid credentials/identification badges and prevent general access to areas with criticality to operations (e.g. computer server rooms, HVAC, chemical storage, or file rooms).

MAY BE FOUND IN:
Law Enforcement
Cybersecurity
Public Works

BUILDING CAPABILITY

AWR-167: Sport Event Risk Management
IS-913.A: Critical Infrastructure Security and Resilience
IS-921.A: Implementing Critical Infrastructure Security and Resilience
MGT335-W: Event Security Planning for Public Safety Professionals

Ohio EMA Training Courses: https://trainingcampus.dps.ohio.gov/CourseMill/pstc/pstc.html
Additional Training Courses: https://www.firstrespondertraining.gov/frt/npcatalog

Examples demonstrate options to consider and are provided for training purposes only. The examples are intended to demonstrate how planning teams may incorporate the key tasks found on FEMA’s Core Capability Development Sheets into planning documents (e.g. the Emergency Operations Plan, Mitigation Plan, Debris Management Plan, HazMat Plan, and so forth). The items in the Functional Areas section are FEMA-identified areas where gaps could exist for the associated core capability.

Counties should not re-design their Emergency Operations Plans around the Core Capabilities; stakeholders should integrate the capabilities within the EOP and in a format that is effective for the jurisdiction.