DOMAINS, TASKS, AND KNOWLEDGE STATEMENTS
BOARD CERTIFIED IN PHYSICAL SECURITY (Note Highlighted Changes)
(Effective November 7, 2011)

Domain I: Physical Security Assessment (33%) **Old Weight (30%)**

Task 01/01: Identify assets to determine their value loss impact and criticality.

Knowledge of:

01/01/01: The nature and types of assets (tangible and intangible)
01/01/02: Valuing various types of assets
01/01/03: Definitions and terminology related to assets, value, loss impact and criticality
01/01/04: Core functions of the place
01/01/05: Current security programs and security management of the place process

REMOVED 01/01/06: Types of security programs and security management processes
REMOVED 01/01/07: Qualitative vs. quantitative risk assessments

Task 01/02: Assess the nature of the threats so that the scope of the problem can be determined.

Knowledge of:

01/02/01: The nature, categories, and types of threats (e.g., natural, man-made)
01/02/02 Different environmental types and severity (e.g., natural disasters, criminal events, terrorism, socio-political, cultural)
01/02/03: Demographics (crime population)
01/02/04: Critical business operations of various types of places or processes
01/02/05: External organizations and their potential impact on facility's security program
01/02/06 Other external factors (legal, loss of reputation, economic, etc) and their impact of the facility's security program

Task 01/03: Conduct a physical security survey in order to identify the vulnerabilities of the organization.

Knowledge of:

01/03/01: Security survey techniques
01/03/02: Qualitative and quantitative risk assessments ***NEW***
01/03/03 Crime prevention through environmental design (CPTED)***NEW***
01/03/04: Situational crime prevention ***New***
01/03/05: Security technologies and equipment applications
01/03/06: Interpretation of building plans, drawings and schematics
01/03/07: Nature and types of data to be collected
01/03/08: Methods of collecting relevant data
01/03/09: Existing equipment, physical security systems, personnel, and procedures
01/03/10: Fault tolerance (i.e. ability of a system to withstand failure) ***NEW***
01/03/11 Applicable standards/regulations/codes and where to find them ***NEW***
01/03/12 Environmental conditions that impact the secuirty level of the place or process ***NEW***

Task 01/04: Perform a risk analysis so that appropriate countermeasures can be developed.

Knowledge of:

01/04/01: Risk analyses strategies and methods
01/04/02: Risk management principles
01/04/03: Methods for analysis and interpretation of collected data
01/04/04: Threat and vulnerability identification ***NEW***
01/04/05: Loss event profile analyses ***NEW***
01/04/06: Methods of evaluating criticality and probability
01/04/07: Appropriate countermeasures related to specific threats
01/04/08: Cost benefit analysis (e.g. return on investment (ROI) analysis, total cost of ownership ***NEW***
01/04/09: Legal issues related to various countermeasures/security applications

Domain II: Application, Design and Integration of Physical Security Systems (38%)   Old Weight (40%)

Task 02/01: Establishing security system requirements and performance specifications

Knowledge of:

02/01/01: Design constraints (e.g. regulations, budget, cost, technical capability, systems design capacities and limitations; materials, equipment and system compatibility
02/01/02: Applicability of risk analysis results ***NEW***
02/01/03: Relevant security terminology and concepts
02/01/04: Applicable codes, standards and guidelines
02/01/05: Methods of setting priorities
02/01/06: Types of security measures
02/01/07: Functional requirements
02/01/08: Performance requirements
02/01/09: Commissioning requirements ***NEW***
02/01/10: Success metrics ***NEW***

Task 02/02: Apply Physical Security Measures and Select Appropriate System Components.

Knowledge of:

02/02/01: Barriers (e.g. fencing, doors, gates, beams, bollards, barriers)
02/02/02: Security Lighting
02/02/03: Biometrics and credentials ***NEW***
02/02/04: Duress systems ***NEW***
02/02/05: Target hardening (e.g. blast mitigation, strategies, ballistic protection ***NEW***
02/02/06: Access control (physical and electronic)
02/02/07: Intrusion detection applications (interior and exterior sensors)
02/02/08: Analog closed circuit television (CCTV)and IP video), cameras, control, recording, storage devices
02/02/09: Personnel, package, and vehicle screening ***NEW***
02/02/10: Emergency notification systems
02/02/11: Security computer systems (hardware, software, peripherals)
02/02/12: Principles of data storage and management ***NEW***
02/02/13: Principles of network infrastructure and network security ***NEW***
02/02/14: Security audio communications (radio, telephone, intercom, IP audio)
02/02/15: Systems monitoring, display and supervision types (field panels, multiplexers, control centers/consoles)
02/02/16: Systems redundancy alternative power sources (battery, UPS, generators**,** surge protection)
02/02/17 Signal and data transmission methods
02/02/18: Equipment and system maintenance requirements ***NEW***
02/02/19: System operations manpower requirements ***NEW***
02/02/20: Identity management (PII) ***NEW***

Task 02/03: Develop and documents system design and pre-implementation plans

Knowledge of:

02/03/01: Design phases (pre-design, schematic design, design development, construction documents and cutover plan)
02/03/02: Design elements (calculations, drawings, specifications, review of manufacturer's submittals and technical data)
02/03/03: Construction specification standards (CSI) ***NEW***
02/03/04: Systems integration (technical approach, connecting with non-security systems)
02/03/05: Project management strategy
02/03/06: Scheduling (Gantt charts, PERT charts, milestones and objectives)
02/03/07: Cost estimates and cost-benefit analysis
02/03/08: Value engineering
02/03/09 Passive and active designs
02/03/10: Major report elements

Domain III: Implementation of Physical Security Measures (29%)   Old Weight (30%)

Task 03/01: Outline criteria for pre-bid meeting to ensure comprehensiveness and appropriateness of implementation.

Knowledge of:

03/01/01: Bid package components
03/01/02: Criteria for evaluation of bids
03/01/03: Technical compliance criteria
03/01/04: Ethics in contracting ***NEW***

Task 03/02: Procure physical security measures and implement recommended quality assurance plan.

Knowledge of:

03/02/01: Project management functions and processes throughout the system life cycle
03/02/02: System integration
03/02/03: Vendor pre-qualification (interviews and due diligence)
03/02/04: Configuration management ***NEW***
03/02/05: Procurement process

Task 03/03: Conduct commissioning, acceptance testing and delivery of the physical security measure.

Knowledge of:

03/03/01: Installation/maintenance inspection techniques
03/03/02: Commissioning
03/03/03: Installation problem resolution (punchlists)
03/03/04: Test and acceptance criteria
03/03/05: Warranty types ***NEW***
03/03/06: End-user training requirements
03/03/07: Ongoing maintenance and inspection requirements