# AMERISTAR®

# ASSA ABLOY

## AFPOP3-2 – Perimeter Security Planning, Site Planning Through Assessment

AIA HSW accredited presentation – 1 hour (CEU)

### SUMMARY

This presentation outlines the steps involved with perimeter site planning and assessment. Moving into identifying layers of security to create a defense-in-depth solution that offers balanced security. Finally, it talks about the solutions that can be incorporated at each perimeter security layer.

### SYNOPSIS

Establishing and maintaining the perimeter of a facility or asset is a key component to an effective physical site security program.  After defining the anticipated threats, physical security products and procedures can be put into place and implemented to better achieve the protection objectives.  Fences, barriers, gates, bollards, pillars, planters, and pedestrian and vehicular access control systems establish the perimeter.  These products can be integrated with intrusion detection sensors, cameras, lighting, and communication equipment to effectively deter, deny, delay, detect, and respond to threats.  Policies can be adopted to address procedural security threats.  Recent product developments (with test video clips), design/build technologies, and procedures will be highlighted and discussed, focusing on holistic approach to physical site security.

The following learning objectives will be met –

Learn Site Planning Assessment – Learn about the three things that need to be identified to conduct a successful Site Planning Assessment: Assets, Threats, and Vulnerabilities.

Learn Risk Evaluation – Once the assessment has been done, the security designer should identify the hazards, which are more vulnerable, assess the likelihood and severity of the risk, and actions to be taken for risk mitigation.

Learn Defense in Depth – After deciding what risks will be handled, the idea is to reduce the likelihood of them happening.  Therefore, we can use an inside-out or outside-in approach to identify the different layers to our disposition to Deter, Deny, Detect, or Delay.

Learn Deter/Deny/Detect/Delay (4 Ds) – Learn the definitions of each of these security strategies.  The idea is for the designers to understand that each solution they implement in the project should add to one of the 4 Ds of Security.

Learn Physical Security Solutions – Learn about the Physical Security Solutions that exist in the market to Deter, Deny, Detect, or Delay.