SSP Instrument

Name of Instrument

Site Security Plan & Alternative Security Program submitted in lieu of the Site Security Plan

Scope of Instrument

The identification and description of how security measures selected by the facility will address the risk-based performance standards listed in 6 CFR 27.230. The RBPS are:

(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility;
(2) Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;
(3) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,
    (i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
    (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and discourages abuse through established disciplinary measures;
(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:
    (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
    (ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
    (iii) Detect attacks at early stages, through counter surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
    (iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning;
(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;
(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;

(7) Sabotage. Deter insider sabotage;
(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;
(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
(10) Monitoring. Maintain effective monitoring, communications and warning systems, including,
    (i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;
    (ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and
    (iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;
(11) Training. Ensure proper security training, exercises, and drills of facility personnel;
(12) Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,
    (i) Measures designed to verify and validate identity;
    (ii) Measures designed to check criminal history;
    (iii) Measures designed to verify and validate legal authorization to work; and
    (iv) Measures designed to identify people with terrorist ties;
(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;
(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;
(16) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
(17) Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards;
(18) Records. Maintain appropriate records; and
(19) Address any additional performance standards the Assistant Secretary may specify

Example of DHS Form used within the scope of this instrument

This instrument collects both SSPs and ASPs submitted in lieu of an SSP. Attached is selected screenshots of DHS Form 9019 through the web portal and is used to standardize the collection of this instrument. DHS Form 9019 identifies most, but not all of the data routinely collected under this instrument. Current version of DHS Form 9019 screenshots may be found at www.dhs.gov/chemicalsecurity.