CSAT Site Security Plan Instrument

Homeland Security

Homeland Security

OMB No. 1670-0007
Expiration Date: April 30, 2016

1. Paperwork Reduction Act Statement

In accordance with the Paperwork Reduction Act, no one is required to respond to a collection of information unless it displays a valid Office of Management and Budget (OMB) Control Number. The valid OMB Control Number for this information collection is 1670-0007. The time required to complete this information collection is estimated to average 18.75 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

2. Survey Selection

In this section, all facilities will choose to proceed with the CSAT SSP or the Alternative Security Program (ASP). Tier 3 and Tier 4 facilities will have, within 90 days of tiering, the option to notify DHS that it intends to submit an Expedited Approval Program (EAP). Facilities that provide this notification would then be allowed to submit an EAP after 30 days of the notification but not later than 120 days of tiering. Facilities that choose to submit an ASP or EAP will complete a manual document and upload. The remainder of this instrument only applies to facilities that choose to do the CSAT SSP.

3. Detection

In this section, the instrument will use yes/no questions, checkboxes, and text fields to collect the following facility and critical asset Detection information:

- Work shifts and the number of employees on each shift
- Intrusion detection system (IDS), any backup power supplies used, sensor type(s), location(s) of the IDS, administration of the IDS system, monitoring frequency, and where it can be controlled
- Type(s) of personnel based monitoring, roving and/or stationed monitoring, locations and frequency of patrols, and observation the posted personnel provides
- Lighting and illumination levels around the facility, and any backup supplies the facility has in place
- Process control functions in place at the facility
- Closed Circuit Television (CCTV) system(s) and their functionality, administration, monitoring frequency, location, and any backup power supplies employed
- Number of onsite security force, their equipment, and response times
- Frequency of formal and informal inventory of the COI
- Planned or proposed detection measures the facility wants to share with the Department including any existing or planned measures the facility proposes to remove or eliminate to include a general timeline for such action

4. Delay

In this section, the instrument will use yes/no questions, checkboxes, and text fields to collect the following facility and critical asset Delay information:

- Location and type of signage, perimeter, gates, doors, barriers, and locking mechanisms
- Clear zone descriptions and standoff distance
- Description of restricted areas/critical assets and policy for accessing critical assets

- Personnel screening performed, identification checks, access control measures used to verify individual identities, escort policies, and restricted area screening types
- Inspection methods of hand carried items, vehicles, trucks, and rail cars
- Access control systems, all backup power supplies, access methods, accountability programs, and compromise procedures
- Key inventory/control programs
- Vehicle access restrictions and identification measures
- "Know Your Customer" or other customer vetting procedures and Product Stewardship programs
- Documentation, review, and validation of Chemical of Interest (COI) sales, purchases , storage, and their distribution
- Carrier and shipment security measures employed
- Man-portable security measures, tamper-evident mechanisms, inventory control methods for tracking, protecting, and the storing of COI and hazardous materials
- Transportation security measures and rail/tanker security storage measures
- Planned or proposed delay measures the facility wants to share with the Department including any existing or planned measures the facility proposes to remove or eliminate to include a general timeline for such action

5. Response

In this section, the instrument will use yes/no questions, checkboxes, and text fields to collect the following facility Response information:

- Emergency and security response capabilities to site emergencies and security events
- Local fire department jurisdiction, police department jurisdiction, HAZMAT team jurisdiction, emergency medical technician (EMT) jurisdiction, and response time
- On-site fire, police, HAZMAT, and EMT capability
- Special response capabilities, ability to shelter-in-place, and any community notification system capability
- Crisis management plan for responding to an incident and all associated plan responsibilities
- Emergency Operations Command Center and Security Command and Control Center
- Communication capabilities for the facility, security, and community
- Facility response equipment maintained and associated backup power
- Frequency of site response drills and exercises, as well as the frequency of other drills and exercise
- Process safeguards and/or automated control systems able of rapidly putting the COI in a safe and stable condition
- Participation in an outreach programs and the frequency
- Participation in joint initiatives, with other organizations/agencies, and the frequency
- Elevated threat level security measures, imminent threat level security measures, time to implement increased levels of security in response to elevating NTAS threat levels, and any additional elevated threat response elements
- Policies, procedures, and training for addressing specific threats as identified by the Assistant Secretary

- Planned or proposed response measures the facility wants to share with the Department including any existing or planned measures the facility proposes to remove or eliminate to include a general timeline for such action

6. Cyber Security

In this section, the instrument will use yes/no questions, checkboxes, and text fields to collect the following facility Cyber Security information:

- Cyber control and business system(s) related to and associated with critical asset(s)
- Physical location of the cyber control and business system(s)
- Development, maintenance, and audits of cyber security policies and procedures
- Personnel security requirements and procedures/practices for facility employees, service providers and other third parties responsible for cyber systems
- IT and cyber security officials and responsibilities
- Cyber access controls and password management
- System boundaries, remote access, cyber security controls and the frequency of network monitoring and event log reviews
- Cyber security training to include topics and frequency
- Cyber security controls, updates, patches, etc.
- Cyber incident response, reporting, recovery/reconstitution phases, etc.
- IT business needs, network/system architecture, and system lifecycle management
- Backup power maintained for cyber/business systems
- Other cyber security measures to include physical access controls
- Planned or proposed cyber security measures the facility wants to share with the Department including any existing or planned measures the facility proposes to remove or eliminate to include a general timeline for such action

7. Security Management

In this section, the instrument will use yes/no questions, checkboxes, and text fields to collect the following facility Security Management information:

- Procedures and policies for the inspection, testing, and periodic maintenance of security equipment and systems to include the types of inspections, testing, and maintenance as well as the frequency of the activities
- Temporary/compensatory measures for security system deficiencies and failures
- Security awareness and training program and drills/exercises for facility personnel, security personnel and SSO/Assistant SSO training with a routine frequency and any programs to reduce workplace violence and potential sabotage
- Personnel surety procedures and background investigations for facility personnel and unescorted visitors with access to restricted areas and critical assets, specifically related to identity, legal authorization to work, and criminal history checks and terrorist tie screening
- Background check audit procedures
- Incident reporting procedures and policies as well as training regarding incident reporting and the frequency in which it takes place
- Security incident investigations including information collected, investigator qualifications, and documentation of past incidents for lessons learned
- Description of the security organization

- Qualifications and responsibilities of the SSO
- Affirmation of the retention and required elements of records associated with training; drills and exercises; incidents and breaches of security; maintenance and testing of security equipment; security threats; audit; Letters of Authorization and Approval; Top-Screen; SVA; SSP and all correspondence with the Department
- Record creation, administration, and disposal
- Planned or proposed security management measures the facility wants to share with the Department including any existing or planned measures the facility proposes to remove or eliminate to include a general timeline for such action