

Security Vulnerability Assessment and Alternative Security Program Submitted in lieu of a Security Vulnerability Assessment

For inclusion within ICR
1670-0007



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 1.41 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.

Chemical of Interest (COI) Selection

In this section, the instrument will give the option for facilities to add Chemicals of Interest (COI) from Appendix A that are not currently Tier 1-4 through a selection list. This allows facilities to voluntarily identify security measures for untiered COI they possess.

COI Use

In this section, for each Tier 1-4 COI and untiered COI identified, the instrument will use Yes/No questions, check boxes, and drop-down menus to collect the following information:

- If the COI is manufactured
- If the COI is sold
- If the COI is shipped and method
- If the COI is received and method

Critical Asset Identification

In this section, the instrument will use text fields and a geospatial tool to collect the following information for critical assets:

- Name and description
- Geospatial location

COI Association

In this section, the instrument will use check boxes to collect which COI is associated with the critical assets identified.

Facility Vulnerability

In this section, the instrument will use text fields and some Yes/No questions to collect the following facility vulnerability information:

- High level critical detection measures and identified vulnerabilities
- High level critical delay measures and identified vulnerabilities
- High level critical response measures and identified vulnerabilities
- High level critical cyber security measures and identified vulnerabilities
- High level critical policies, procedures, and resources and identified vulnerabilities
- The facility's threat and risk assessment efforts, if applicable

- Whether or not the facility has identified all potential vulnerabilities in their current security posture, including any planned improvements in order to meet the applicable Risk Based Performance Standards