CSAT Security Vulnerability Assessment

Questions

June 2008

Version 1.0

Homeland Security

General

Paperwork Burden Disclosure Notice:

The public reporting burden for this form is estimated to be 250 hours. The burden estimate includes time for reviewing instructions, researching existing data sources, gathering and maintaining the needed data, and completing and submitting the form. You may send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: NPPD/OIP/Infrastructure Security Compliance Division, Attention: Dennis Deziel, Project Manager, U.S. Department of Homeland Security, Mail Stop 8100, Washington, DC 20528-8100.

(OMB Control No. (1670-0007)). Your completion of the CSAT Security Vulnerability Assessment is mandatory according to Public Law 109- 295 Section 550. You are not required to respond to this collection of information (i.e., the CSAT SVA) unless a valid OMB control number is displayed. NOTE: DO NOT send the completed CSAT SVA to the above address.

Submission Statement:

My statements in this submission are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Enter the facility identification number from the DHS Initial Notification Letter.
[Q:1.01-3311]

Does the DHS Initial Notification letter indicate that the facility is a Tier 4 facility?
[Q:1.01-3314]

- ○ Yes
- ○ No

Facility Information

Facility Name

[Note: The address should be the facility's physical location. This may be different from the mailing address.]

Facility Location Address

Facility Location Address (continued)

Facility Location Address (continued)

Facility Location City

Facility Location State

Facility Location ZIP Code

Facility Coordinates

Facility Latitude

Facility Longitude

Submit ASP Document

As detailed in CFATS, facilities with a Tier 4 ranking have the option of either completing and submitting an SVA using the CSAT SVA, or uploading an Alternate Security Program (ASP) in lieu of an SVA. If a Tier 4 facility elects to submit an ASP, rather than complete the CSAT SVA, this section describes the process to upload the relevant files (ASP documentation and site plans or maps) into the CSAT SVA tool.

If the facility is not Tier 4, skip the ASP section questions and go to ***Facility Security Information*** *(page 10).*

Do you want to upload an alternate security program (ASP) in lieu of performing a CSAT SVA? (If you select *No*, you will be directed to the process for completing and submitting a CSAT SVA.)
[Q:1.05-3315]

- ○ Yes
- ○ No

If No, skip the ASP Documents questions and go to ***Facility Security Information*** *(page 10).*

ASP Documents

The alternate security program (ASP) documentation that you upload should satisfy the following factors that are conditions for completeness.

Does the ASP cover all of the facility assets that are associated with the security issues and chemicals of interest specified in the DHS Initial Notification letter?
[Q:1.1-3316]

- ○ Yes
- ○ No

Does the ASP use a Center for Chemical Process Safety (CCPS)-approved methodology?
[Q:1.1-11671]

- ○ Yes
- ○ No

Does the ASP address the asset characterization factors described in 6 CFR 27.215?
[Q:1.1-11672]

- ○ Yes
- ○ No

▲ Asset Characterization includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection. See 6 CFR 27.

Does the ASP address the threat assessment factors described in 6 CFR 27.215?
[Q:1.1-11673]

- ○ Yes
- ○ No

▲ Threat assessment includes a description of possible internal threats, external threats, and internally-assisted threats. See 6 CFR 27.

Does the ASP cover all of the applicable attack modes covered in the CSAT SVA?
[Q:1.1-3317]

- ○ Yes
- ○ No

▲ See the CFATS CVI Document Repository for the list of attack modes covered in the CSAT SVA.

Does the ASP address the countermeasures factors described in 6 CFR 27.215?
[Q:1.1-11674]

- ○ Yes
- ○ No

▲ Security vulnerability analysis includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards. See 6 CFR 27.

Does the ASP address the risk assessment requirements described in 6 CFR 27.215?
[Q:1.1-11675]

- ○ Yes
- ○ No

▲ Risk assessment includes a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of the success of an attack. See 6 CFR 27.

If “Yes” selected for any of the ASP document questions, skip the next question.

ASP Does Not Address All of the Factors

The ASP does not address all of the factors in 6 CFR 27. Do you still want to upload the ASP for consideration? (If you select “No,” you will be directed to the process for completing and submitting a CSAT SVA.)

Continue ASP Upload Process? [Q:1.12-12451]

- ○ Yes
- ○ No

*If “No” go to **Facility Security Information** (page 10).*

Enter the name of the non-CSAT security vulnerability methodology.
[Q:1.13-3320]

What is the date of the non-CSAT security vulnerability assessment?
[Q:1.13-3331]

▲ The response format is **mm/dd/yyyy**.
(e.g. May 1, 2006 is entered as 05/01/2006.)

Upload ASP Documents

Enter names for the ASP files to upload.
Enter a brief description of the uploaded ASP file.

ASP Files [Q:1.14-6911]	Brief description of the ASP file. [Q:1.15-6912]

Upload Plot Plans/Maps

Are the locations of assets that were analyzed in the ASP for each COI and security issue marked on the plot plans/maps?
[Q:1.2-3351]

- ○ Yes
- ○ No

Names of Plot Plans/Maps.
Enter the image width and image height in miles.

Enter names for the ASP plot plan/map files to upload.

Ensure that the locations of assets that were analyzed in the ASP for each COI and security issue are marked on the plot plans/maps. If necessary, include within the map a legend to icons/assets that are used in the plot plans/maps.

Plot Plan/Map Name to Upload [Q:1.3-3354]	**Image width (miles):** [Q:1.31-3356]	**Image height (miles):** [Q:1.31-3357]

To complete a CSAT SVA, go to page 10.

Facility Security Information

DHS Initial Notification Letter – Security Issues

Please use the DHS Initial Notification Letter to answer the following questions.

Does the DHS Initial Notification Letter indicate that the facility should address security issues related to release-toxic COI?
[Q:2.0 -971]

- ○ Yes
- ○ No

Does the DHS Initial Notification letter indicate that the facility should address security issues related to release-flammable COI?
[Q:2.0 -3131]

- ○ Yes
- ○ No

Does the DHS Initial Notification letter indicate that the facility should address security issues related to release-explosive COI?
[Q:2.0 -3132]

- ○ Yes
- ○ No

Does the DHS Initial Notification letter indicate that the facility should address security issues related to theft-EXP/IEDP COI?
[Q:2.0 -3172]

- ○ Yes
- ○ No

Does the DHS Initial Notification letter indicate that the facility should address security issues related to theft-WME COI?
[Q:2.0 -3171]

- ○ Yes
- ○ No

Does the DHS initial notification letter indicate that the facility should address security issues related to theft-CW/CWP COI?
[Q:2.0 -3151]

- ○ Yes
- ○ No

Does the DHS Initial Notification letter indicate that the facility should address security issues related to sabotage/contamination COI?
[Q:2.0 -3173]

- ○ Yes
- ○ No

Release Toxic Chemicals of Interest

Indicate which release toxic chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Release Flammable Chemicals of Interest (page 16).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.1-1037]	
		Yes	No
Acrolein [2-Propenal or Acrylaldehyde]	107-02-8	○	○
Allyl alcohol [2-Propen-1-ol]	107-18-6	○	○
Ammonia (anhydrous)	7664-41-7	○	○
Ammonia (conc. 20% or greater)	7664-41-7	○	○
Arsenic trichloride [Arsenous trichloride]	7784-34-1	○	○
Arsine	7784-42-1	○	○
Boron trichloride [Borane, trichloro]	10294-34-5	○	○
Boron trifluoride [Borane, trifluoro]	7637-07-2	○	○
Boron trifluoride compound with methyl ether (1:1) [Boron, trifluoro [oxybis (methane)]-, T-4-]	353-42-4	○	○
Bromine	7726-95-6	○	○
Carbon disulfide	75-15-0	○	○
Chlorine	7782-50-5	○	○
Chlorine dioxide [Chlorine oxide, ClO_2]	10049-04-4	○	○
Chloroform [Methane, trichloro-]	67-66-3	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.1-1037]	
		Yes	No
Chloromethyl ether [Methane, oxybis(chloro-)]	542-88-1	○	○
Chloromethyl methyl ether [Methane, chloromethoxy-]	107-30-2	○	○
Cyanogen chloride	506-77-4	○	○
Cyclohexylamine [Cyclohexanamine]	108-91-8	○	○
Diborane	19287-45-7	○	○
Epichlorohydrin [Oxirane, (chloromethyl)-]	106-89-8	○	○
Ethylenediamine [1,2-Ethanediamine]	107-15-3	○	○
Fluorine	7782-41-4	○	○
Formaldehyde (solution)	50-00-0	○	○
Hydrochloric acid (conc. 37% or greater)	7647-01-0	○	○
Hydrocyanic acid	74-90-8	○	○
Hydrofluoric acid (conc. 50% or greater)	7664-39-3	○	○
Hydrogen chloride (anhydrous)	7647-01-0	○	○
Hydrogen fluoride (anhydrous)	7664-39-3	○	○
Hydrogen sulfide	7783-06-4	○	○
Isobutyronitrile [Propanenitrile, 2-methyl-]	78-82-0	○	○
Isopropyl chloroformate [Carbonochloridic acid, 1-methylethyl ester]	108-23-6	○	○
Methacrylonitrile [2-Propenenitrile, 2-methyl-]	126-98-7	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.1-1037]	
		Yes	No
Methyl hydrazine [Hydrazine, methyl-]	60-34-4	○	○
Methyl isocyanate [Methane, isocyanato-]	624-83-9	○	○
Methyl thiocyanate [Thiocyanic acid, methyl ester]	556-64-9	○	○
Nitric acid	7697-37-2	○	○
Nitric oxide [Nitrogen oxide (NO)]	10102-43-9	○	○
Oleum (Fuming Sulfuric acid) [Sulfuric acid, mixture with sulfur trioxide]	8014-95-7	○	○
Perchloromethylmercaptan [Methanesulfenyl chloride, trichloro-]	594-42-3	○	○
Phosgene [Carbonic dichloride] or [carbonyl dichloride]	75-44-5	○	○
Phosphorus oxychloride [Phosphoryl chloride]	10025-87-3	○	○
Phosphorus trichloride	7719-12-2	○	○
Propionitrile [Propanenitrile]	107-12-0	○	○
Propyleneimine [Aziridine, 2-methyl-]	75-55-8	○	○
Sulfur dioxide (anhydrous)	7446-09-5	○	○
Sulfur tetrafluoride [Sulfur fluoride (SF_4), (T-4)-]	7783-60-0	○	○
Sulfur trioxide	7446-11-9	○	○
Tetramethyllead [Plumbane, tetramethyl-]	75-74-1	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.1-1037]	
		Yes	No
Titanium tetrachloride [Titanium chloride ($TiCl_4$) (T-4)-]	7550-45-0	○	○

Release Flammable Chemicals of Interest

Indicate which release flammable chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Release Explosive Chemicals of Interest (page 22).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Acetaldehyde	75-07-0	○	○
Acetylene [Ethyne]	74-86-2	○	○
Acrylonitrile [2-Propenenitrile]	107-13-1	○	○
Acrylyl chloride [2-Propenoyl chloride]	814-68-6	○	○
Allylamine [2-Propen-1-amine]	107-11-9	○	○
Bromotrifluorethylene [Ethene, bromotrifluoro-]	598-73-2	○	○
1,3-Butadiene	106-99-0	○	○
Butane	106-97-8	○	○
Butene	25167-67-3	○	○
1-Butene	106-98-9	○	○
2-Butene	107-01-7	○	○
2-Butene-cis	590-18-1	○	○
2-Butene-trans [2-Butene, (E)]	624-64-6	○	○
Carbon oxysulfide [Carbon oxide sulfide (COS); carbonyl sulfide]	463-58-1	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Chlorine monoxide [Chlorine oxide]	7791-21-1	○	○
1-Chloropropylene [1-Propene, 1-chloro-]	590-21-6	○	○
2-Chloropropylene [1-Propene, 2-chloro-]	557-98-2	○	○
Crotonaldehyde [2-Butenal]	4170-30-3	○	○
Crotonaldehyde, (E)- [2-Butenal], (E)-]	123-73-9	○	○
Cyanogen [Ethanedinitrile]	460-19-5	○	○
Cyclopropane	75-19-4	○	○
Dichlorosilane [Silane, dichloro-]e	4109-96-0	○	○
Difluoroethane [Ethane, 1,1-difluoro-]	75-37-6	○	○
Dimethylamine [Methanamine, N-methyl-]	124-40-3	○	○
Dimethyldichlorosilane [Silane, dichlorodimethyl-]	75-78-5	○	○
1,1-Dimethylhydrazine [Hydrazine, 1, 1-dimethyl-]	57-14-7	○	○
2,2-Dimethylpropane [Propane, 2,2-dimethyl-]	463-82-1	○	○
Ethane	74-84-0	○	○
Ethyl acetylene [1-Butyne]	107-00-6	○	○
Ethyl chloride [Ethane, chloro-]	75-00-3	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Ethyl ether [Ethane, 1,1-oxybis-]	60-29-7	○	○
Ethyl mercaptan [Ethanethiol]	75-08-1	○	○
Ethyl nitrite [Nitrous acid, ethyl ester]	109-95-5	○	○
Ethylamine [Ethanamine]	75-04-7	○	○
Ethylene [Ethene]	74-85-1	○	○
Ethylene oxide [Oxirane]	75-21-8	○	○
Ethyleneimine [Aziridine]	151-56-4	○	○
Furan	110-00-9	○	○
Hydrazine	302-01-2	○	○
Hydrogen	1333-74-0	○	○
Hydrogen selenide	7783-07-5	○	○
Iron, pentacarbonyl- [Iron carbonyl ($Fe(CO)_5$), (TB5-11)-]	13463-40-6	○	○
Isobutane [Propane, 2-methyl]	75-28-5	○	○
Isopentane [Butane, 2-methyl-]	78-78-4	○	○
Isoprene [1,3-Butadiene, 2-methyl-]	78-79-5	○	○
Isopropyl chloride [Propane, 2-chloro-]	75-29-6	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Isopropylamine [2-Propanamine]	75-31-0	○	○
Methane	74-82-8	○	○
2-Methyl-1-butene	563-46-2	○	○
3-Methyl-1-butene	563-45-1	○	○
Methyl chloride [Methane, chloro-]	74-87-3	○	○
Methyl chloroformate [Carbonochloridic acid, methyl ester]	79-22-1	○	○
Methyl ether [Methane, oxybis-]	115-10-6	○	○
Methyl formate [Formic acid Methyl ester]	107-31-3	○	○
Methyl mercaptan [Methanethiol]	74-93-1	○	○
Methylamine [Methanamine]	74-89-5	○	○
2-Methylpropene [1-Propene, 2-methyl-]	115-11-7	○	○
Methyltrichlorosilane [Silane, trichloromethyl-]	75-79-6	○	○
Nickel Carbonyl	13463-39-3	○	○
1,3-Pentadiene	504-60-9	○	○
Pentane	109-66-0	○	○
2-Pentene, (E)-	646-04-8	○	○
2-Pentene, (Z)-	627-20-3	○	○
Peracetic acid [Ethaneperoxic acid]	79-21-0	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Phosphine	7803-51-2	○	○
Piperidine	110-89-4	○	○
Propadiene [1,2-Propadiene]	463-49-0	○	○
Propane	74-98-6	○	○
Propyl chloroformate [Carbonchloridic acid, propylester]	109-61-5	○	○
Propylene [1-Propene]	115-07-1	○	○
Propylene oxide [Oxirane, methyl-]	75-56-9	○	○
Propyne [1-Propyne]	74-99-7	○	○
Silane	7803-62-5	○	○
Tetrafluoroethylene [Ethene, tetrafluoro-]	116-14-3	○	○
Tetramethylsilane [Silane, tetramethyl-]	75-76-3	○	○
Tetranitromethane [Methane, tetranitro-]	509-14-8	○	○
Trichlorosilane [Silane, trichloro-]	10025-78-2	○	○
Trifluorochloroethylene [Ethene, chlorotrifluoro]	79-38-9	○	○
Trimethylamine [Methanamine, N,N-dimethyl-]	75-50-3	○	○
Trimethylchlorosilane [Silane, chlorotrimethyl-]	75-77-4	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.2-1038]	
		Yes	No
Vinyl acetate monomer [Acetic acid ethenyl ester]	108-05-4	○	○
Vinyl acteylene [1-Buten-3-yne]	689-97-4	○	○
Vinyl chloride [Ethene, chloro-]	75-01-4	○	○
Vinyl ethyl ether [Ethene, ethoxy-]	109-92-2	○	○
Vinyl fluoride [Ethene, fluoro-]	75-02-5	○	○
Vinyl methyl ether [Ethene, methoxy-]	107-25-5	○	○
Vinylidene chloride [Ethene, 1,1-dichloro-]	75-35-4	○	○
Vinylidene fluoride [Ethene, 1,1-difluoro-]	75-38-7	○	○
Fuels: Bunker fuel		○	○
Fuels: Diesel		○	○
Fuels: Gasoline		○	○
Fuels: Home heating oil		○	○
Fuels: JP A (jet fuel)		○	○
Fuels: JP 5 (jet fuel)		○	○
Fuels: JP 8 (jet fuel)		○	○
Fuels: Kerosene		○	○
Fuels: LPG		○	○

Release Explosive Chemicals of Interest

Indicate which release explosive chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Theft/Diversion Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest (page 25).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.3-1039]	
		Yes	No
Ammonium nitrate, [with more than 0.2 percent combustible substances, including any organic substance calculated as carbon, to the exclusion of any other added substance]	6484-52-2	○	○
Ammonium perchlorate	7790-98-9	○	○
Ammonium picrate	131-74-8	○	○
Barium azide	18810-58-7	○	○
Diazodinitrophenol	87-31-0	○	○
Diethyleneglycol dinitrate	693-21-0	○	○
Dingu [Dinitroglycoluril]	55510-04-8	○	○
Dinitrophenol	25550-58-7	○	○
Dinitroresorcinol	519-44-8	○	○
Dipicryl sulfide	2217-06-3	○	○
Dipicrylamine [or] Hexyl [Hexanitrodiphenylamine]	131-73-7	○	○
Guanyl nitrosaminoguanylidene hydrazine		○	○
Hexanitrostilbene	20062-22-0	○	○
Hexolite [Hexotol]	121-82-4	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.3-1039]	
		Yes	No
HMX [Cyclotetramethylene-tetranitramine]	2691-41-0	○	○
Lead azide	13424-46-9	○	○
Lead styphnate [Lead trinitroresorcinate]	15245-44-0	○	○
Mercury fulminate	628-86-4	○	○
5-Nitrobenzotriazol	2338-12-7	○	○
Nitrocellulose	9004-70-0	○	○
Nitroglycerine	55-63-0	○	○
Nitromannite [Mannitol hexanitrate, wetted]	15825-70-4	○	○
Nitrostarch	9056-38-6	○	○
Nitrotriazolone	932-64-9	○	○
Octolite	57607-37-1	○	○
Octonal	78413-87-3	○	○
Pentolite	8066-33-9	○	○
PETN [Pentaerythritol tetranitrate]	78-11-5	○	○
Picrite [Nitroguanidine]	556-88-7	○	○
RDX [Cyclotrimethylenetrinitramine]	121-82-4	○	○
RDX and HMX mixtures	121-82-4	○	○
Tetranitroaniline	53014-37-2	○	○
Tetrazene [Guanyl nitrosaminoguanyltetrazene]	109-27-3	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.3-1039]	
		Yes	No
1H-Tetrazole	288-94-8	○	○
TNT [Trinitrotoluene]	118-96-7	○	○
Torpex [Hexotonal]	67713-16-0	○	○
Trinitroaniline	26952-42-1	○	○
Trinitroanisole	606-35-9	○	○
Trinitrobenzene	99-35-4	○	○
Trinitrobenzenesulfonic acid	2508-19-2	○	○
Trinitrobenzoic acid	129-66-8	○	○
Trinitrochlorobenzene	88-88-0	○	○
Trinitrofluorenone	129-79-3	○	○
Trinitro-meta-cresol	602-99-3	○	○
Trinitronaphthalene	55810-17-8	○	○
Trinitrophenetole	4732-14-3	○	○
Trinitrophenol	88-89-1	○	○
Trinitroresorcinol	82-71-3	○	○
Tritonal	54413-15-9	○	○

Theft/Diversion Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest

Indicate which theft/diversion EXP/IEDP chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Theft/Diversion Weapon of Mass Effect (WME) Chemicals of Interest (page 29).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.4-1043]	
		Yes	No
Aluminum (powder)	7429-90-5	○	○
Ammonium nitrate, [with more than 0.2 percent combustible substances, including any organic substance calculated as carbon, to the exclusion of any other added substance]	6484-52-2	○	○
Ammonium nitrate, solid [nitrogen concentration of 23% nitrogen or greater]	6484-52-2	○	○
Ammonium perchlorate	7790-98-9	○	○
Ammonium picrate	131-74-8	○	○
Barium azide	18810-58-7	○	○
Diazodinitrophenol	87-31-0	○	○
Diethyleneglycol dinitrate	693-21-0	○	○
Dingu [Dinitroglycoluril]	55510-04-8	○	○
Dinitrophenol	25550-58-7	○	○
Dinitroresorcinol	519-44-8	○	○
Dipicryl sulfide	2217-06-3	○	○
Dipicrylamine [or] Hexyl [Hexanitrodiphenylamine]	131-73-7	○	○
Guanyl nitrosaminoguanylidene hydrazine		○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.4-1043]	
		Yes	No
Hexanitrostilbene	20062-22-0	○	○
Hexolite [Hexotol]	121-82-4	○	○
HMX [Cyclotetramethylene-tetranitramine]	2691-41-0	○	○
Hydrogen peroxide (concentration of at least 35%)	7722-84-1	○	○
Lead azide	13424-46-9	○	○
Lead styphnate [Lead trinitroresorcinate]	15245-44-0	○	○
Magnesium (powder)	7439-95-4	○	○
Mercury fulminate	628-86-4	○	○
Nitric acid	7697-37-2	○	○
Nitrobenzene	98-95-3	○	○
5-Nitrobenzotriazol	2338-12-7	○	○
Nitrocellulose	9004-70-0	○	○
Nitroglycerine	55-63-0	○	○
Nitromannite [Mannitol hexanitrate, wetted]	15825-70-4	○	○
Nitromethane	75-52-5	○	○
Nitrostarch	9056-38-6	○	○
Nitrotriazolone	932-64-9	○	○
Octolite	57607-37-1	○	○
Octonal	78413-87-3	○	○
Pentolite	8066-33-9	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.4-1043]	
		Yes	No
PETN [Pentaerythritol tetranitrate]	78-11-5	○	○
Phosphorus	7723-14-0	○	○
Picrite [Nitroguanidine]	556-88-7	○	○
Potassium chlorate	3811-04-9	○	○
Potassium nitrate	7757-79-1	○	○
Potassium perchlorate	7778-74-7	○	○
Potassium permanganate	7722-64-7	○	○
RDX [Cyclotrimethylenetrinitramine]	121-82-4	○	○
RDX and HMX mixtures	121-82-4	○	○
Sodium azide	26628-22-8	○	○
Sodium chlorate	7775-09-9	○	○
Sodium nitrate	7631-99-4	○	○
Tetranitroaniline	53014-37-2	○	○
Tetrazene [Guanyl nitrosaminoguanyltetrazene]	109-27-3	○	○
1H-Tetrazole	288-94-8	○	○
TNT [Trinitrotoluene]	118-96-7	○	○
Torpex [Hexotonal]	67713-16-0	○	○
Trinitroaniline	26952-42-1	○	○
Trinitroanisole	606-35-9	○	○
Trinitrobenzene	99-35-4	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.4-1043]	
		Yes	No
Trinitrobenzenesulfonic acid	2508-19-2	○	○
Trinitrobenzoic acid	129-66-8	○	○
Trinitrochlorobenzene	88-88-0	○	○
Trinitrofluorenone	129-79-3	○	○
Trinitro-meta-cresol	602-99-3	○	○
Trinitronaphthalene	55810-17-8	○	○
Trinitrophenetole	4732-14-3	○	○
Trinitrophenol	88-89-1	○	○
Trinitroresorcinol	82-71-3	○	○
Tritonal	54413-15-9	○	○

Theft/Diversion Weapon of Mass Effect (WME) Chemicals of Interest

Indicate which theft/diversion WME chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest (page 32).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.5-1042]	
		Yes	No
Arsine	7784-42-1	○	○
Boron tribromide	10294-33-4	○	○
Boron trichloride [Borane, trichloro]	10294-34-5	○	○
Boron trifluoride [Borane, trifluoro]	7637-07-2	○	○
Bromine chloride	13863-41-7	○	○
Bromine trifluoride	7787-71-5	○	○
Carbonyl fluoride	353-50-4	○	○
Carbonyl sulfide	463-58-1	○	○
Chlorine	7782-50-5	○	○
Chlorine pentafluoride	13637-63-3	○	○
Chlorine trifluoride	7790-91-2	○	○
Cyanogen [Ethanedinitrile]	460-19-5	○	○
Cyanogen chloride	506-77-4	○	○
Diborane	19287-45-7	○	○
Dichlorosilane [Silane, dichloro-]	4109-96-0	○	○
Dinitrogen tetroxide	10544-72-6	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.5-1042]	
		Yes	No
Fluorine	7782-41-4	○	○
Germane	7782-65-2	○	○
Germanium tetrafluoride	7783-58-6	○	○
Hexaethyl tetraphosphate and compressed gas mixtures	757-58-4	○	○
Hexafluoroacetone	684-16-2	○	○
Hydrogen bromide (anhydrous)	10035-10-6	○	○
Hydrogen chloride (anhydrous)	7647-01-0	○	○
Hydrogen cyanide [Hydrocyanic acid]	74-90-8	○	○
Hydrogen fluoride (anhydrous)	7664-39-3	○	○
Hydrogen iodide, anhydrous	10034-85-2	○	○
Hydrogen selenide	7783-07-5	○	○
Hydrogen sulfide	7783-06-4	○	○
Methyl mercaptan [Methanethiol]	74-93-1	○	○
Methylchlorosilane	993-00-0	○	○
Nitric oxide [Nitrogen oxide (NO)]	10102-43-9	○	○
Nitrogen trioxide	10544-73-7	○	○
Nitrosyl chloride	2696-92-6	○	○
Oxygen difluoride	7783-41-7	○	○
Perchloryl fluoride	7616-94-6	○	○
Phosgene [Carbonic dichloride] or [carbonyl dichloride]	75-44-5	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.5-1042]	
		Yes	No
Phosphine	7803-51-2	○	○
Phosphorus trichloride	7719-12-2	○	○
Selenium hexafluoride	7783-79-1	○	○
Silicon tetrafluoride	7783-61-1	○	○
Stibine	7803-52-3	○	○
Sulfur dioxide (anhydrous)	7446-09-5	○	○
Sulfur tetrafluoride [Sulfur fluoride (SF_4), (T-4)-]	7783-60-0	○	○
Tellurium hexafluoride	7783-80-4	○	○
Titanium tetrachloride [Titanium chloride ($TiCl_4$) (T-4)-]	7550-45-0	○	○
Trifluoroacetyl chloride	354-32-5	○	○
Trifluorochloroethylene [Ethene, chlorotrifluoro]	79-38-9	○	○
Tungsten hexafluoride	7783-82-6	○	○

Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest

Indicate which theft/diversion CW/CWP chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Sabotage/Contamination Chemicals of Interest (page 35).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.6-1041]	
		Yes	No
Arsenic trichloride [Arsenous trichloride]	7784-34-1	○	○
1,4-Bis(2-chloroethylthio)-n-butane	142868-93-7	○	○
Bis(2-chloroethylthio)methane	63869-13-6	○	○
Bis(2-chloroethylthiomethyl)ether	63918-90-1	○	○
1,5-Bis(2-chloroethylthio)-n-pentane	142868-94-8	○	○
1,3-Bis(2-chloroethylthio)-n-propane	63905-10-2	○	○
2-Chloroethylchloro-methylsulfide	2625-76-5	○	○
Chlorosarin [o-Isopropyl methylphosphonochloridate]	1445-76-7	○	○
Chlorosoman [o-Pinacolyl methylphosphonochloridate]	7040-57-5	○	○
DF [Methyl phosphonyl difluoride]	676-99-3	○	○
N,N-(2-diethylamino)ethanethiol	100-38-9	○	○
o,o-Diethyl S-[2-(diethylamino)ethyl] phosphorothiolate	78-53-5	○	○
Diethyl methylphosphonite	15715-41-0	○	○
N,N-Diethyl phosphoramidic dichloride	1498-54-0	○	○
N,N-(2-diisopropylamino)ethanethiol [N,N-diisopropyl-β-aminoethane thiol]	5842-07-9	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.6-1041]	
		Yes	No
N,N-Diisopropyl phosphoramidic dichloride	23306-80-1	○	○
N,N-(2-dimethylamino)ethanethiol	108-02-1	○	○
N,N-Dimethyl phosphoramidic dichloride [Dimethylphosphoramido-dichloridate]	677-43-0	○	○
N,N-(2-dipropylamino)ethanethiol	5842-06-8	○	○
N,N-Dipropyl phosphoramidic dichloride	40881-98-9	○	○
Ethyl phosphonyl difluoride	753-98-0	○	○
Ethyldiethanolamine	139-87-7	○	○
Ethylphosphonothioic dichloride	993-43-1	○	○
HN1 (Nitrogen Mustard-1) [Bis(2-chloroethyl)ethylamine]	538-07-8	○	○
HN2 (Nitrogen Mustard-2) [Bis(2-chloroethyl)methylamine]	51-75-2	○	○
HN3 (Nitrogen Mustard-3) [Tris(2-chloroethyl)amine]	555-77-1	○	○
Isopropylphosphonothioic dichloride	1498-60-8	○	○
Isopropylphosphonyl difluoride	677-42-9	○	○
Lewisite 1 [2-chlorovinyldichloroarsine]	541-25-3	○	○
Lewisite 2 [Bis(2-chlorovinyl)chloroarsine]	40334-69-8	○	○
Lewisite 3 [Tris(2-chlorovinyl)arsine]	40334-70-1	○	○
MDEA [Methyldiethanolamine]	105-59-9	○	○
Methylphosphonothioic dichloride	676-98-2	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.6-1041]	
		Yes	No
O-Mustard (T) [Bis(2-chloroethylthioethyl)ether]	63918-89-8	○	○
Nitrogen mustard hydrochloride [Bis(2-chloroethyl)methylamine hydrochloride]	55-86-7	○	○
Phosphorus oxychloride [Phosphoryl chloride]	10025-87-3	○	○
Propylphosphonothioic dichloride	2524-01-8	○	○
Propylphosphonyl difluoride	690-14-2	○	○
QL [o-Ethyl-o-2-diisopropylaminoethyl methylphosphonite]	57856-11-8	○	○
Sarin [o-Isopropyl methylphosphonofluoridate]	107-44-8	○	○
Sesquimustard [1,2-Bis(2-chloroethylthio)ethane]	3563-36-8	○	○
Soman [o-Pinacolyl methylphosphonofluoridate]	96-64-0	○	○
Sulfur Mustard (Mustard gas (H)) [Bis(2-chloroethyl)sulfide]	505-60-2	○	○
Tabun [o-Ethyl-N,N-dimethylphosphoramido-cyanidate]	77-81-6	○	○
Thiodiglycol [Bis(2-hydroxyethyl)sulfide]	111-48-8	○	○
Triethanolamine	102-71-6	○	○
Triethanolamine hydrochloride	637-39-8	○	○
Triethyl phosphite	122-52-1	○	○
Trimethyl phosphite	121-45-9	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.6-1041]	
		Yes	No
VX [o-Ethyl-S-2-diisopropylaminoethyl methyl phosphonothiolate]	50782-69-9	○	○

Sabotage/Contamination Chemicals of Interest

Indicate which sabotage/contamination chemicals of interest are listed in the DHS Initial Notification Letter.

If answered No for all chemicals, go to Facility Characteristics (page 39).

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.7-1671]	
		Yes	No
Acetone cyanohydrin, stabilized	75-86-5	○	○
Acetyl bromide	506-96-7	○	○
Acetyl chloride	75-36-5	○	○
Acetyl iodide	507-02-8	○	○
Allyltrichlorosilane, stabilized	107-37-9	○	○
Aluminum bromide, anhydrous	7727-15-3	○	○
Aluminum chloride, anhydrous	7446-70-0	○	○
Aluminum phosphide	20859-73-8	○	○
Amyltrichlorosilane	107-72-2	○	○
Antimony pentafluoride	7783-70-2	○	○
Boron tribromide	10294-33-4	○	○
Bromine pentafluoride	7789-30-2	○	○
Bromine trifluoride	7787-71-5	○	○
Butyltrichlorosilane	7521-80-4	○	○
Calcium hydrosulfite [Calcium dithionite]	15512-36-4	○	○
Calcium phosphide	1305-99-3	○	○
Chlorine dioxide [Chlorine oxide, (ClO_2)]	10049-04-4	○	○
Chloroacetyl chloride	79-04-9	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.7-1671]	
		Yes	No
Chlorosulfonic acid	7790-94-5	○	○
Chromium oxychloride	14977-61-8	○	○
Cyclohexyltrichlorosilane	98-12-4	○	○
Diethyldichlorosilane	1719-53-5	○	○
Dimethyldichlorosilane [Silane, dichlorodimethyl-]	75-78-5	○	○
Diphenyldichlorosilane	80-10-4	○	○
Dodecyltrichlorosilane	4484-72-4	○	○
Ethyltrichlorosilane	115-21-9	○	○
Fluorosulfonic acid	7789-21-1	○	○
Hexyltrichlorosilane	928-65-4	○	○
Iodine pentafluoride	7783-66-6	○	○
Lithium amide	7782-89-0	○	○
Lithium nitride	26134-62-3	○	○
Magnesium diamide	7803-54-5	○	○
Magnesium phosphide	12057-74-8	○	○
Methyldichlorosilane	75-54-7	○	○
Methylphenyldichlorosilane	149-74-6	○	○
Methyltrichlorosilane [Silane, trichloromethyl-]	75-79-6	○	○
Nonyltrichlorosilane	5283-67-0	○	○
Octadecyltrichlorosilane	112-04-9	○	○
Octyltrichlorosilane	5283-66-9	○	○
Phenyltrichlorosilane	98-13-5	○	○

Chemical Name	CAS#	Was the chemical listed in the letter? [Q:2.7-1671]	
		Yes	No
Phosphorus oxychloride [Phosphoryl chloride]	10025-87-3	○	○
Phosphorus pentabromide	7789-69-7	○	○
Phosphorus pentachloride	10026-13-8	○	○
Phosphorus pentasulfide	1314-80-3	○	○
Phosphorus trichloride	7719-12-2	○	○
Potassium cyanide	151-50-8	○	○
Potassium phosphide	20770-41-6	○	○
Propyltrichlorosilane	141-57-1	○	○
Silicon tetrachloride	10026-04-7	○	○
Sodium cyanide	143-33-9	○	○
Sodium hydrosulfite [Sodium dithionite]	7775-14-6	○	○
Sodium phosphide	12058-85-4	○	○
Strontium phosphide	12504-16-4	○	○
Sulfuryl chloride	7791-25-5	○	○
Thionyl chloride	7719-09-7	○	○
Titanium tetrachloride [Titanium chloride ($TiCl_4$) (T-4)-]	7550-45-0	○	○
Trichlorosilane [Silane, trichloro-]	10025-78-2	○	○
Trimethylchlorosilane [Silane, chlorotrimethyl-]	75-77-4	○	○
Vinyltrichlorosilane	75-94-5	○	○
Zinc hydrosulfite [Zinc dithionite]	7779-86-4	○	○

Facility Characteristics

What is the surrounding topography of the facility?
[Q:2.92-5911]

Note: Only answer if the facility has issues related to toxic chemicals.

- ○ Urban
- ○ Rural

▲ Select the option, **Urban** or **Rural**, that best defines the area surrounding the facility. The entry here should match the corresponding entry in the CSAT Top-Screen. As in the Top-Screen, if a facility is covered by EPA's Risk Management Plan, the selection of urban or rural should be consistent with the facility's current RMP on file with EPA. If a facility is not covered by a current RMP and the terrain surrounding the facility varies depending on the approach to the facility, select the topography (urban or rural) that is most representative of the facility's location. If still unsure, select Rural.

Is the facility located on a navigable waterway?
[Q:2.92-3313]

- ○ Yes
- ○ No

▲ Facilities should answer *Yes* to this question if a waterway along any portion of the facility perimeter can accommodate small to large watercraft. This includes vessels ranging from small pleasure craft, barges, and deep draft vessels. Facilities responding *No* will not evaluate a Maritime attack mode as part of the vulnerability analysis because it is not applicable for this facility.

Security Equipment at the Facility

List the types of security equipment that help to reduce the vulnerability of COI at the facility.

List any security equipment at the facility that helps reduce the vulnerability of COI that the DHS Initial Notification letter noted as contributing to a high level of security risk. List only security equipment that applies across the facility, as opposed to a specific COI or asset. See the SVA Instructions document for examples of responses.

If you have multiple entries of the same type or need more space, copy the following page as necessary.

Security Equipment [Q:2.93-8331]	Location [Q:2.93-8332]	Support System Required [Q:2.93-8333]
CCTV monitoring systems for COI areas		
Intrusion detection system for facility perimeter		
Intrusion detection system with 24-hour monitoring		
Security response team		
Security response vehicles		
Security communications system		
Redundant security communications systems		
Vehicle screening at access point for dangerous materials		
Personal screening at access points for dangerous materials		
Other:		

Utility Systems and Infrastructure Support

List below any utility systems or other infrastructure support required for the security equipment and the location of the systems or equipment. See the SVA Instructions document for examples of responses.

Select an item from the list, and complete the utility systems or infrastructure support information. Add entries until all applicable items have been provided. If the facility has none of the utility systems or infrastructure support systems shown in the list, leave this question blank.

If you have multiple entries of the same type or need more space, copy this page as necessary.

System/Infrastructure [Q:2.94-8351]	**Location** [Q:2.94-8352]
Electric power system	
Redundant offsite electric power sources	
Backup AC power system from onsite generators	
Backup DC power system from UPS equipment	
Other:	
Electric power system	
Redundant offsite electric power sources	
Backup AC power system from onsite generators	
Backup DC power system from UPS equipment	
Other:	

Inventory Control

If the facility does not have any Theft/Diversion chemicals present, go to Personnel Access Control Measures at the Facility (page 47).

List any inventory control measures used at the facility that would help reduce vulnerability to theft/diversion. If the facility does not have any inventory control measures, leave this question blank. For each identified inventory control measure, complete additional questions.

Inventory Control/Measures
[Q:2.95-8371]

Copy the Inventory Control Pages as necessary to answer for all controls/measures listed here.

Copy the following Inventory Control/Measure pages (43-46), fill in the control/measure you are answering questions for here, and then answer the questions regarding that specific Control/Measure.

Inventory Control/Measure
[Q:2.95-8371]

Inventory Control - Details

Please note if the inventory control measure is automated, the frequency with which it is applied, the location of the measure, the inventory features, and whether the features apply to the COI. See the SVA Instruction document for examples of responses.

Is the inventory measure automated?
[Q:2.951-8711]

- ○ Yes
- ○ No

Frequency Applied
[Q:2.951-8372]

- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ Quarterly
- ○ Semi-annually
- ○ Annually
- ○ Other

Location
[Q:2.951-8373]

Select all the features that apply to this Control Measure.

Inventory Control Feature	Is the feature used in this control measure? [Q:2.951-12191]	
Continuous electronic inventory accounting for all COI	Yes	No
Periodic electronic inventory accounting for all COI	Yes	No
Periodic, manual inventory accounting for all COI	Yes	No
Recordkeeping procedures that track customer orders	Yes	No
Recordkeeping procedures that identify suspicious orders and inquiries	Yes	No
Recordkeeping procedures that report inventory discrepancies to regulatory and/or law enforcement agencies	Yes	No
Restricted access to customer ordering system	Yes	No
Restricted access to customer information	Yes	No
Training for customer sales representatives on handling suspicious orders or inquiries	Yes	No
Background checks for customer sales representatives	Yes	No
Inventory reconciliation procedures	Yes	No
Inventory reconciliation procedures that identify, investigate, and resolve shortages	Yes	No
Procedures for reporting shortages to regulatory and/or law enforcement agencies	Yes	No
Product segregation procedures	Yes	No
Restricted access to segregated products	Yes	No

Enter the chemicals present at the facility in the appropriate list.

Theft/Diversion Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.951-8511] Yes	No
		○	○
		○	○
		○	○

Theft/Diversion Weapon of Mass Effect (WME) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.951-8571] Yes	No
		○	○
		○	○
		○	○

Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.951-8573] Yes	No
		○	○
		○	○
		○	○

Personnel Access Control Measures at the Facility

List below any personnel access control measures used at the facility that could help reduce vulnerability to an attack. See the Instructions document for examples of responses.

Complete the applicable personnel access control measure information. If the facility has none of the personnel access control measures shown in the drop-down list, leave this question blank.

- **Personnel recognition by officer** - Access control system based on personnel recognition by security officer with no picture or electronic badge
- **Manual badge validation by officer** - Access control system with manual badge validation by security officer
- **Biometric validation** - Access control system with biometric validation
- **Computerized access with no validation** - Access control system with computerized access with no validation (e.g., swipe or proximity card system with no guard or computer validation process)
- **Personnel access allowed on foot only** - Personnel access allowed on foot only (i.e., employee and visitor vehicles not allowed inside facility process boundary)

Copy the following page as needed to answer all personnel access control measures at the facility. Use the blank space provided under Access Control Measure to answer with one that is not listed.

Access Control Measure [Q:2.96-8431]	Is the control measure automated? [Q:2.94-8351]	Frequency Applied [Q:2.94-8432]	Location [Q:2.94-8433]	Personnel Covered [Q:2.94-8434]
○ Personnel recognition by officer ○ Manual badge validation by officer ○ Biometric validation ○ Computerized access with no validation ○ Personal access allowed on foot only ○ Visitor access clearance and badging ○ Visitors require advance registration ○ Visitors require full time escort Other:	○ Yes ○ No	○ Daily ○ Weekly ○ Monthly ○ Quarterly ○ Semi-annually ○ Annually ○ Other		

Shipping and Receiving Control Measures at the Facility

If the facility does not have any Theft/Diversion or Sabotage chemicals present, go to Post-Release Measures and Equipment (page 54).

List below any shipping and receiving measures at the facility that would be useful in reducing vulnerability to an attack. If the facility does not have any shipping and receiving measures, leave this question blank. For each identified shipping and receiving measure, complete additional questions.

Control Measures
[Q:2.97-8611]

Copy the Shipping and Receiving Control Measures as necessary to answer regarding all control measures listed here.

Copy the following Control Measure pages (50-53), fill in the control/measure you are answering questions for here, and then answer the questions regarding that specific Control Measure.

Control Measure
[Q:2.97-8611]

Shipping and Receiving Control Measures – Details

Please note if the shipping and receiving inventory control measure is automated, the frequency with which it is applied, the location of the measure, the inventory features, and whether the features apply to the COI. See the Instruction Guide for examples of responses.

Is the control measure automated?
[Q:2.971-8719]

- ○ Yes
- ○ No

Frequency Applied
[Q:2.971-8612]

- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ Quarterly
- ○ Semi-annually
- ○ Annually
- ○ Other

Location
[Q:2.971-8613]

Select all the features that apply to this Control Measure.

Control Measure Feature	Is the feature used in this control measure? [Q:2.971-12171]	
Restricted access to shipping and receiving area	○ Yes	○ No
Restricted access to staging area for shipments	○ Yes	○ No
Reconciliation of outbound shipments with customer orders	○ Yes	○ No
Reconciliation of intra-company shipments	○ Yes	○ No

Control Measure Feature	Is the feature used in this control measure? [Q:2.971-12171]	
Reconciliation of intra-company receipts	Yes	No
Confirm receipt of customer's orders	Yes	No
Confirm receipt of intra-company shipments	Yes	No
Confirm receipt of intra-company receipts	Yes	No
Customer verification procedures that validate new customers' business and product end-use	Yes	No
Customer verification procedures that periodically validate established customer's business and product end-use	Yes	No
Customer verification procedures that include on-site visit(s) to customer facility	Yes	No
Training for shipping and receiving personnel on validating the accuracy and completeness of receipts and shipments	Yes	No
Training for shipping and receiving personnel on securing the shipping and receiving area	Yes	No
Background check on shipping and receiving personnel	Yes	No

Theft/Diversion Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.971-8659] Yes	No

Theft/Diversion Weapon of Mass Effect (WME) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.971-8571] Yes	No
		○	○
		○	○
		○	○

Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.971-8666] Yes	No
		○	○
		○	○
		○	○

Sabotage/Contamination Chemicals of Interest

Chemical Name	CAS#	Does the measure apply to COI? [Q:2.971-8671]	
		Yes	No
		○	○
		○	○
		○	○

Post-Release Measures and Equipment

List below any post-release measures or equipment that would be considered useful in reducing the consequence of a release-toxic COI release. Do not list mitigation systems that only apply to a single asset (e.g., a secondary containment dike around toxic liquid storage). See the SVA Instructions document for examples of responses.

Select applicable items from the list, and complete the post-release measures or equipment information. If the facility has none of the post-release measures or equipment shown, leave this question blank.

If you have multiple entries of the same type or need more space, copy the following page as necessary.

Post-Release Equipment/Application [Q:2.98-8451]	**Location** [Q:2.98-8452]	**Support Systems Required** [Q:2.98-8453]
○ Community emergency warning system – telephone auto-dialer		
○ Community emergency warning system – community sirens		
○ Community outreach on evacuation/sheltering (if warning system provided)		
Other:		

○ Community emergency warning system – telephone auto-dialer		
○ Community emergency warning system – community sirens		
○ Community outreach on evacuation/sheltering (if warning system provided)		
Other:		

Site Vulnerability Factors

List below any facility features, offsite terrain, or infrastructure items that potentially increase the site's vulnerability to attack. See the Instructions document for examples of responses.

Enter the site vulnerability, and complete the information. Continue adding entries until all applicable items have been provided. If the facility has no site vulnerabilities, leave this question blank.

Site Vulnerability [Q:2.99-8454]	Comment [Q:2.99-84545]

Asset Characterization

Facility Assets

Identify one or more assets for each COI.

Each COI described in the facility's DHS initial notification letter must have one or more assets defined (i.e., each COI must be listed as a primary COI for at least one asset). A primary COI is the COI for which the consequences of damage to that asset will be estimated. As each asset can have only one primary COI associated with it, an asset that is associated with more than one COI might need to be defined multiple times, listing each COI as primary.

For example: The user has a building housing COI "x" and "y".

- Asset 1 would be the building and list the primary COI as "x".
- Asset 2 would be the same building but list the primary COI as "y".

Also, if a COI presents two separate security issues (e.g., release toxic and theft) separate assets need to be defined for each security issue and the primary security issue for each asset must be specified. The primary security issue is the security issue for which the vulnerability and consequence associated with attacks on the asset are estimated.

The asset names should be distinct enough to identify the asset. This field can be up to 34 characters in length. A suggestion would be to include the equipment, primary COI and/or primary security issue (e.g., Bulk Storage Tank 1103-Chem X).

Include all applicable assets have been provided. Then describe each asset and provide the requested information. See the SVA Instructions document for information on asset selection.

Asset Name

Facility Assets - Description

Enter a brief description of the asset.

Provide a brief description of the asset including:

- **The primary function (e.g., storage, production, loading/unloading);**
- **Number and type of grouped or interconnected vessels; and**
- **Any additional facility identifying number or name. (For example, *raw material storage area, including two storage tanks T-1 and T-2*)**

[Q:3.2-3831]

Enter the Primary COI for this asset.

Primary Security Issue For This Asset

Indicate which primary security issue the Primary COI belongs to.
Select only one primary security issue.

Select the primary security issue that will be examined for this asset (i.e., the security issue for which the vulnerability and consequence analyses for this asset apply). If there are two or more security issues associated with COI that pertain to this asset, separate assets must be defined for each security issue/COI combination. See the SVA Instructions document for additional information.

- ○ Release of Toxic COI [Q:3.2-10211]
- ○ Release of Flammable COI [Q:3.2-10212]
- ○ Release of Explosive CO I [Q:3.2-10213]
- ○ Theft/Diversion of Explosive/IEDP COI [Q:3.2-10214]
- ○ Theft/Diversion of WME COI [Q:3.2-10215]
- ○ Theft/Diversion of CW/CWP COI [Q:3.2-10216]
- ○ Sabotage/Contamination of COI [Q:3.2-10217]

Facility Assets - Detail

Is there a cyber control system related to this asset?
[Q:3.56-3659]

- ○ Yes
- ○ No

▲ These cyber control systems should be limited to those systems that have the ability to control the process and could result in a release or contamination. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

If Primary COI is Theft/Diversion, answer the following question.

Is there a cyber business system related to this asset?
[Q:3.561-4292]

- ○ Yes
- ○ No

▲ Examples include business management systems like SAP™ or inventory management systems.

Facility Asset Directions

Answer the questions regarding the chemicals of interest present at the asset (pages 59-60).

If the Primary COI is Release, answer the containment type questions on page 61.

If the Primary COI is Release-Toxic, answer the storage questions on page 62 and the mitigation questions on pages 63-65.

If the Primary COI is Theft/Diversion, answer the packaging detail questions on page 66.

After all of your assets have been listed, complete the questions about cyber control systems on page 67 and cyber business systems on page 68 for each system you have present. If none, leave those questions blank.

Enter in all chemicals of interest (COI) associated with this asset. Be sure to include the Primary COI listed above.
Enter the quantity of each chemical of interest associated with this asset (pounds).
Is the Theft/Diversion chemical shipped offsite from this asset?

Round the quantity to two significant digits (e.g., round 247500 pounds to 250000 pounds, and round 7625 pounds to 7600 pounds). Do not use commas when entering data.

Toxic Chemicals of Interest	Quantity (pounds)	Facility's largest inventory of the COI?	
		Yes	No
		○	○
		○	○
		○	○

Flammable Chemicals of Interest	Quantity (pounds)	Yes	No
		○	○
		○	○
		○	○

Explosive Chemicals of Interest	Quantity (pounds)	Yes	No
		○	○
		○	○
		○	○

Theft/Diversion Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest	Quantity (pounds)	Facility's largest inventory of the COI?		Shipped Offsite?	
		Yes	No	Yes	No
		○	○	○	○
		○	○	○	○
		○	○	○	○

Theft/Diversion Weapon of Mass Effect (WME) Chemicals of Interest	Quantity (pounds)	Yes	No	Yes	No
		○	○	○	○
		○	○	○	○
		○	○	○	○

Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest	Quantity (pounds)	Yes	No	Yes	No
		○	○	○	○
		○	○	○	○
		○	○	○	○

Sabotage/Contamination Chemicals of Interest	Quantity (pounds)	Yes	No
		○	○
		○	○
		○	○

Release Chemicals of Interest

Check the items below where the COI is located or contained within this asset. Check all that apply.
[Q:3.31-5472]

Containment Type	Is the containment type used for this asset? [Q:3.31-12192]	
Barge	Yes	No
Cylinder	Yes	No
Isotainer	Yes	No
Low Pressure Storage Tank	Yes	No
Mounded Storage	Yes	No
Pipeline	Yes	No
Piping	Yes	No
Pressure Vessel	Yes	No
Process Unit	Yes	No
Rail Car	Yes	No
Reactor	Yes	No
Spheres	Yes	No
Tank Trunk	Yes	No
Tube Trailers	Yes	No
Underground Storage	Yes	No
Other	Yes	No

Toxic Chemicals of Interest

Select the predominant chemical phase of the chemical at this asset.
Select liquid for the predominant phase if the chemical is a liquid at or near atmospheric temperature and pressure.

If the Toxic COI is process/stored as a gas, leave the other questions in this table blank.

Enter the liquid process or storage temperature and pressure of the toxic COI. Enter the maximum height of the liquid in the vessel. Indicate whether the liquid is an aqueous solution. Enter the initial percent concentration by weight of the toxic chemical in aqueous solution associated with this asset.

If the Toxic COI liquid is not an aqueous solution, skip the concentration percentage by weight question.

Chemical Name	Process/Storage Condition [Q:3.41-6993]	Temperature (degree Fahrenheit) [Q:3.412-6995]	Process or storage pressure (psig) [Q:3.412-8893]	Liquid height (feet) [Q:3.412-8894]	Percent Concentration by Weight [Q:3.413-7011]
	○ Gas ○ Liquid ○ Pressurized Liquefied Gas ○ Refrigerated Liquefied Gas				
	○ Gas ○ Liquid ○ Pressurized Liquefied Gas ○ Refrigerated Liquefied Gas				

Primary Release Toxic

Mitigation measures in place that you expect to help mitigate a toxic release (check all that apply):

- ☐ Dike, berm, or other similar containment [Q:3.42-10471]
- ☐ Leak detection system [Q:3.42-10472]
- ☐ Fixed vapor suppression system [Q:3.42-10473]
- ☐ Notification system for offsite evacuation or sheltering in place [Q:3.42-10474]
- ☐ Other measures [Q:3.42-10475]

Toxic Release – Mitigation

Dike, berm, or other similar containment

Description of containment
[Q:3.421-9211]

Containment area (sq ft) [Q:3.421-9212]

Containment capacity (gallons) [Q:3.421-9213]

Leak detection system (e.g., fixed chemical detectors with alarm)

Description of system
[Q:3.421-9214]

Estimated time to detection for a toxic release (minutes) [Q:3.421-9215]

Fixed vapor suppression system (e.g., foam or dry chemical cover,

Description of system
[Q:3.421-9216]

Estimated time to activation for a toxic release (minutes) [Q:3.421-9218]

Estimated vapor reduction for a toxic release (%) [Q:3.421-9219]

Notification system for offsite evacuation or sheltering in place (e.g.,

Description of system
[Q:3.421-9220]

Estimated time to activation of system (minutes) [Q:3.421-9221]

Description of community outreach/training on evacuation and sheltering in place
[Q:3.421-9222]

Other measures

Description of other measures
[Q:3.421-9223]

Description of mitigation provided by this measure for a toxic release
[Q:3.421-9224]

Theft/Diversion Primary COI

Provide the following information for all instances of the COI listed above at this asset.

For facilities with multiple instances of the COI at the asset, enter the first instance and complete the related questions. Continue adding entries until all applicable instances have been provided.

Concentration range (% by weight) [Q:3.48-9011, Q:3.5-9096, Q:3.52-9171]	**Packaging type description** [Q:3.48-9031, Q:3.5-9097, Q:3.52-9172]	**Transportation packaging type** [Q:3.48-9032, Q:3.5-9098, Q:3.52-9174]	**Total quantity of COI in this transportation packaging type (lbs)** [Q:3.48-9091, Q:3.5-9165, Q:3.52-9173]
○ 0 – 30% ○ 31 – 50% ○ 51 – 80% ○ 81 – 100%		○ Portable ○ Bulk Storage ○ Bulk Transportation	
○ 0 – 30% ○ 31 – 50% ○ 51 – 80% ○ 81 – 100%		○ Portable ○ Bulk Storage ○ Bulk Transportation	
○ 0 – 30% ○ 31 – 50% ○ 51 – 80% ○ 81 – 100%		○ Portable ○ Bulk Storage ○ Bulk Transportation	

Cyber Control Systems

List the cyber control systems that are associated with assets that have been identified. Enter cyber control system description. Indicate which assets are associated with the system.

These cyber control systems should be limited to those systems that have the ability to control the process and could result in a release or contamination. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

Control System Name [Q:3.7-3711]	Control System Description [Q:3.71-3719]	Assets controlled by this system. [Q:3.71-3835]

Cyber Business Systems

List the cyber business systems that are associated with assets that have been identified. Enter cyber control system description. Indicate which assets with theft/diversion as their primary COI are associated with the system.

Possible examples of these types of systems include business management systems like SAP or inventory management systems.

Business System Name [Q:3.8-3715]	Control System Description [Q:3.81-3720]	Assets controlled by this system. [Q:3.81-3837]

Vulnerability Analysis

Answer the following scenarios based on what type of primary COI you have selected for the asset. Use the following tables to determine what sections should be answered for a specific asset. Copy the pages needed as necessary. Only fill out the Maritime section if the facility is located on a navigable waterway (page 39) [Q:2.92-3313]. Only fill out the Diversion section if the facility ships the Primary-COI offsite (page 60). For example, if you have an asset with a primary toxic COI, fill out the Aircraft, Maritime (if on waterway), Vehicle, Assault Team, and Standoff Attack Scenarios. Then for the Aircraft Attack Scenario, fill out the sections regarding Identifiability Probability, Achievability Probability, and Availability Probability. Be sure to fill out the attack description for each attack scenario indicated in the Attack Scenario Table.

The online application requires the user to annotate the CSAT facility imagery (or upload and annotate imagery for the facility), to indicate each asset location, attack location, and the radius of the damage zone for each scenario.

Asset Name

Attack Scenarios

		Aircraft	Maritime only if facility is on navigable waterway (page 39) [Q:2.92-3313]	Vehicle	Assault Team	Standoff	Theft	Diversion only if Primary COI shipped offsite (page 60)	Sabotage
Release	Toxic (include the Mitigation Measures page with these attack scenarios)	X	X	X	X	X			
	Flammable	X	X	X	X	X			
	Explosive	X	X	X	X	X			

		Aircraft	Maritime only if facility is on navigable waterway (page 39) [Q:2.92-3313]	Vehicle	Assault Team	Standoff	Theft	Diversion only if Primary COI shipped offsite (page 60)	Sabotage
Theft/ Diversion	EXP/IEDP						X	X	
	WME						X	X	
	CW/CWP						X	X	
	Sabotage								X

Attack Scenario Descriptions

		Aircraft	Maritime only if facility is on navigable waterway (page 39) [Q:2.92-3313]	Vehicle	Assault Team	Standoff	Theft	Diversion only if Primary COI shipped offsite (page 60)	Sabotage
Vulnerability Questions	Identifiability Probability	X	X	X	X	X	X		X
	Accessibility Probability		X	X	X	X	X		X
	Facility Security Response Force Capability		X	X	X		X		X
	Offsite Security Response Force Capability		X	X	X		X		X
	Achievability Probability	X	X	X	X	X	X		X
	Target Hardness Probability		X	X	X	X			X
	Availability Probability	X	X	X	X	X	X		X
	Unauthorized Customer Registration							X	
	Unauthorized Order Placement							X	

		Aircraft	Maritime only if facility is on navigable waterway (page 39) [Q:2.92-3313]	Vehicle	Assault Team	Standoff	Theft	Diversion only if Primary COI shipped offsite (page 60)	Sabotage
	Unauthorized Order Pickup (if customer is allowed to pick up orders at the asset) [Q:12.6-7736]							X	

Aircraft Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

○ A1 - Medium-range, medium-lift aircraft (i.e., 737 size) crashes into facility in attempt to destroy large storage tanks of COI located in the tank farm area, separate from other process equipment.

○ A2 - Adversary crashes medium-range, medium-lift aircraft (i.e., 737 size) into facility in attempt to destroy large chemical processing area containing a variety of process equipment, including in-process inventories of COI.

○ Other – user-defined aircraft scenario.

Annotate a plot of the site to indicate the asset and a 950 foot damage radius surrounding the asset attacked in the scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.
[Q:9.01-7588]

What is the expected number of people at the facility within the outer damage radius (950 feet)?

Expected number of people includes the number of employees or contractors that would be in the specified area of the explosion based on the assumptions for the scenario (e.g., random time, shift change, at night, weekend, holiday).

[Q:9.21-4063]

Fill in quantities of the appropriate COI that match the same chemical list as the primary COI.

Calculate the quantity using the same counting rules provided by CFATS for calculating the STQs for the applicable release chemicals of interest.

Enter all quantities (pounds) of the same release COI within the inner damage radius (490 feet).

Primary COI Name	CAS#	Quantity (pounds) [Q:9.3-9706]

Enter quantities of all release-flammable COI within the inner damage radius (490 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:9.4-9738]

Enter quantities of all release-explosive COI within the inner damage radius (490 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:9.5-9743]

Maritime Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ○ B1 - Adversary drives boat carrying IED on an offsite waterway that comes within the proximity of the asset and explodes the boat at the closest approach point to the asset
- ○ B2 - Adversary drives boat carrying IED into an onsite waterway or channel that comes within the proximity of the asset and explodes the boat at the closest approach point to the asset.
- ○ Other – user-defined maritime scenario.

Annotate a plot of the site to indicate the location of the boat when the attack takes place, the location of the asset, and the inner and outer (140 and 270 foot) damage radii surrounding the asset attacked in the scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.
[Q:7.01-7275]

Is any portion of the asset within the inner damage radius (140 feet)?

- ○ Yes
- ○ No

If Yes, answer the following questions and answer the attack scenario descriptions associated with this asset.

What is the expected number of people at the facility within the outer damage radius (270 feet)?

Expected number of people includes the number of employees or contractors that would be in the specified area of the explosion based on the assumptions for the scenario (e.g., random time, shift change, at night, weekend, holiday).

[Q:7.21-3896]

Calculate the quantity using the same counting rules provided by CFATS for calculating the STQs for the applicable release chemicals of interest.

Fill in quantities of the appropriate COI that match the same chemical list as the primary COI.

Enter all quantities (pounds) of the same release COI within the inner damage radius (140 feet).

Primary COI Name	CAS#	Quantity (pounds) [Q:7.3-9170]

Enter quantities of all release-flammable COI within the inner damage radius (140 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:7.4-9226]

Enter quantities of all release-explosive COI within the inner damage radius (140 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:7.5-9228]

Vehicle Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ○ V1 - Adversary places VBIED outside of the facility perimeter, but located close enough for the vehicle bomb to destroy the COI storage tank or area considered the asset.
- ○ V2 - The adversary cuts the facility back gate open during off hours (i.e., night or weekend operation) and drives the VBIED to a location at the end of the secondary containment closest to tank/area that is this asset.
- ○ V3 - The adversary accesses the facility with a VBIED by entering the plant site behind a vehicle making an authorized entry or by crashing through a controlled access gate. The adversary drives the VBIED to the storage area or process unit that represents this asset and detonates the device there.
- ○ Other – user-defined vehicle scenario.

Annotate a plot of the site to indicate the location of the vehicle when the attack takes place, the location of the asset, and the inner and outer (170 and 340 foot) damage radii surrounding the asset attacked in the scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.
[Q:8.01-7563]

Is any portion of the asset within the inner damage radius (170 feet)?

- ○ Yes
- ○ No

If Yes, answer the follow questions and answer the attack scenario descriptions associated with this asset.

What is the expected number of people at the facility within the outer damage radius (340 feet)?

Expected number of people includes the number of employees or contractors that would be in the specified area of the explosion based on the assumptions for the scenario (e.g., random time, shift change, at night, weekend, holiday).

[Q:8.21-3995]

Calculate the quantity using the same counting rules provided by CFATS for calculating the STQs for the applicable release chemicals of interest.

Fill in quantities of the appropriate COI that match the same chemical list as the primary COI.

Enter all quantities (pounds) of the same release COI within the inner damage radius (170 feet).

Primary COI Name	CAS#	Quantity (pounds) [Q:8.3-9636]

Enter quantities of all release-flammable COI within the inner damage radius (170 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:8.4-9668]

Enter quantities of all release-explosive COI within the inner damage radius (170 feet).

Chemical Name	CAS#	Total Quantity (pounds) [Q:8.5-9673]

Assault Team Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ○ AT1 - Adversary team climbs or cuts the facility perimeter fence and places two explosive charges against the asset.
- ○ AT2 - Adversary assault team attacks security assets at access control point and then moves through the plant on foot and places two explosive charges on this asset.
- ○ Other – user-defined assault team scenario.

Annotate a plot of the site to indicate the asset and a 110 foot damage radius surrounding the asset attacked in the scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.
[Q:10.01-7613]

What is the expected number of people at the facility within the outer damage radius (110 feet)?

Expected number of people includes the number of employees or contractors that would be in the specified area of the explosion based on the assumptions for the scenario (e.g., random time, shift change, at night, weekend, holiday).

[Q:10.21-4080]

Fill in quantities of the appropriate COI that match the same chemical list as the primary COI.

Calculate the quantity using the same counting rules provided by CFATS for calculating the STQs for the applicable release chemicals of interest.

Enter all quantities (pounds) of the same release COI within the inner damage radius (55 feet).

Primary COI Name	CAS#	Quantity (pounds) [Q:10.3-9793]

Enter quantities of all release-flammable COI within the inner damage radius (55 feet).

Chemical Name	CAS#	Quantity (pounds) [Q:10.4-9825]

Enter quantities of all release-explosive COI within the inner damage radius (55 feet).

Chemical Name	CAS#	Quantity (pounds) [Q:10.5-9830]

Standoff Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ○ SO1 - The adversary accesses the facility and fires the stand-off weapon (i.e., light anti-tank weapon with shaped charge warhead) into the asset from a distance no greater than 200 meters initiating a release of a COI.
- ○ SO2 - The facility is surrounded by a contiguous 7ft. in height chain-link fence. Asset is within 100 meters of the facility perimeter and is easily visible from outside the fence. The adversary drives a van or delivery truck into the parking lot of an adjacent facility and uses the top of the vehicle as an elevated platform to launch a stand-off weapon (i.e., light anti-tank weapon with shaped charge warhead) at the asset from a distance of 100 to 200 meters.
- ○ Other – user-defined standoff scenario.

Annotate a plot of the site to indicate the location of the asset, the location from which the standoff attack takes place, and a 657 foot range radius centered on the location of the standoff weapon.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.
[Q:11.01-7631]

Is any portion of the asset within the range of the standoff weapon (657 feet)?

- ○ Yes
- ○ No

If No and answering for a Primary-Toxic COI attack description, skip the mitigation measures questions.

Sabotage Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ○ SA1 - Adversary (insider or outsider) accesses a placarded amount of a sabotage/contamination COI that is destined for shipment and contaminates the shipment in a manner that will result in an explosion or release once shipped from the facility.
- ○ SA2 - Adversary (insider or outsider) accesses a placarded amount of a sabotage/contamination COI destined for shipment and tampers with the shipment. The tampering results in an explosion or release once shipped from the facility.
- ○ Other – user-defined sabotage scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.

Answer the following questions relating to the primary COI.

Quantity of COI at Risk in this scenario (pounds)
[Q:13.2-11372]

Percent Concentration by Weight in this scenario
[Q:13.2-11373]

Theft Scenario

○ T1 - Adversary team enters the facility and steals largest portable package, leaving the facility in a vehicle without immediate awareness by facility staff (i.e., no immediate law enforcement notification and pursuit).

○ T2 - Adversary team enters the facility in a vehicle, obtains one or more portable package of the theft COI, and successfully leaves the facility in the vehicle without being detected.

○ T3 - Adversary enters the facility on foot and steals one or more man-portable package, moving them to transport vehicles outside of the facility.

○ Other – user-defined theft scenario.

If Other, describe the scenario.

Describe the attack scenario relevant to this asset.

Answer the following questions relating to the primary COI.

Quantity of COI at Risk in this scenario (pounds)
[Q:12.2-11343]

Percent Concentration by Weight in this scenario
[Q:12.2-11344]

Diversion Scenario

Is the customer permitted to pick up orders at this asset?
[Q:12.6-7736]

- ○ Yes
- ○ No

Composite Diversion Scenario, consisting of any of these three elements:

- **Adversary is allowed to register as a customer to purchase COI and have it shipped to the adversary's chosen location, or**
- **Adversary is allowed to file a false order for an existing customer that results in shipping the COI container to a location that is not controlled by the approved customer, or**
- **Adversary is allowed to accept shipment of or pick up an order of the COI that is intended for an approved customer.**

Answer the following questions relating to the primary COI.

Quantity of COI at Risk in this scenario (pounds)
[Q:12.7-11351]

Percent Concentration by Weight in this scenario
[Q:12.7-11352]

Mitigation Measures only apply to attack scenarios for assets the have toxic as their primary COI.

Mitigation Measures

Mitigation Measures in place that you expect to help mitigate this scenario.

Answer the questions relevant to what mitigation measures you indicated were present at this asset.

Dike, berm, or other similar containment

Does the dike or berm containment survive the attack?
[Q:7.3-9177,Q:8.3-9637,Q:9.3-9707, Q:10.3-9794, Q:11.3-9974]

- ○ Yes
- ○ No

Leak detection system (e.g., fixed chemical detectors with alarm)

Does the leak detection system survive the attack?
[Q:7.3-9191, Q:8.3-9638,Q:9.3-9708, Q:10.3-9795, Q:11.3-9975]

- ○ Yes
- ○ No

Fixed vapor suppression system (e.g., foam or dry chemical cover, water spray system)

Does the vapor suppression system survive the attack?
[Q:7.3-9192, Q:8.3-9639,Q:9.3-9709, Q:10.3-9796, Q:11.3-9976]

- ○ Yes
- ○ No

Notification system for offsite evacuation or sheltering in place (e.g., phone dialing system, alarm system)

Does the offsite notification system survive the attack?
[Q:7.3-9193, Q:8.3-9640,Q:9.3-9710, Q:10.3-9797, Q:11.3-9977]

- ○ Yes
- ○ No

Other Mitigation Measures

Does the other mitigation measure survive the attack?
[Q:7.3-9194, Q:8.3-9641, Q:9.3-9711, Q:10.3-9798, Q:11.3-9978]

- ○ Yes
- ○ No

Identifiability Probability

This refers to the probability that the adversary can identify the specific target asset during the course of planning and executing an attack. Identifiability is a function of the size, labeling, and nature of the asset and its similarity to others at the facility.

When estimating identifiability, a facility should consider it difficult for an adversary to distinguish between several similar items of equipment, only some of which would be viable targets. Labeling of equipment is also a factor in this assessment.

How likely is the adversary, in the course of planning and/or executing this attack scenario against this asset, to identify the specific asset(s) that must be attacked or stolen to achieve significant consequences?
[Q:7.22-7276, Q:8.22-9609, Q:9.22-9687, Q:10.22-9767, Q:11.22-9900, Q:12.22-7657, Q:13.22-9948]

- ○ a. Adversary is extremely unlikely to successfully identify the specific asset they desire to attack during this scenario. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to successfully identify the specific asset they desire to attack during this scenario. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in identifying the specific target in the scenario. Prob(0.4 to 0.6)
- ○ d. Adversary success in identifying the specific target in the scenario is likely. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to successfully identify the specific asset they desire to attack during this scenario. Prob(0.8 to 1.0)

Identifiability assumptions:
[Q:7.22-7277, Q:8.22-9610, Q:9.22-9688, Q:10.22-9768, Q:11.22-9901, Q:12.22-7658, Q:13.22-9949]

Accessibility Probability

This refers to the probability that an adversary is successful in reaching the location that they must access to successfully execute an attack, given the security measures currently implemented at the facility (not counting facility or offsite security force response capability).

This factor should reflect the ability of existing security systems and processes (without counting for response force actions) to prevent the adversary from reaching a location close enough to the asset to launch the specific type of attack (i.e., close enough to place an explosive device or use a standoff weapon).

How likely do you think that the adversary would be in successfully breaching existing security measures and accessing a location from which they can attack the asset?
[Q:7.22-7371, Q:8.22-9611, Q:10.22-9769, Q:11.22-9902, Q:12.22-7659, Q:13.22-9950]

- ○ a. Adversary is extremely unlikely to successfully access the asset. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to successfully access the asset. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in accessing this asset with this attack. Prob(0.4 to 0.6)
- ○ d. Adversary is likely to successfully access the asset. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to successfully access the asset. Prob(0.8 to 1.0)

Accessibility assumptions:
[Q:7.22-7372, Q:8.22-9612, Q:10.22-9769, Q:11.22-9903, Q:12.22-7659, Q:13.22-9951]

Facility Security Response Force Capability

This refers to the probability that a facility (i.e., onsite) security response force (if any) is able to interdict an adversary force before it succeeds in executing an attack (assuming the security measures alone were not adequate).

This vulnerability factor reflects the ability of the onsite security force to intervene in time to stop a specific type of attack. Assume that the accessibility controls discussed above would not have stopped the adversary, but would have offered a delay consistent with the types of physical security measures at the facility.

How likely is the facility security response force to successfully interdict the adversary before they are successful in executing their attack (assuming that other security measures alone are not successful in stopping the attack)?
[Q:7.22-7391, Q:8.22-9613, Q:10.22-9771, Q:12.22-7661, Q:13.22-9952]

- ○ a. Facility security response force is almost certain to successfully interdict this type of attack. Prob(0.8 to 1.0)
- ○ b. Facility security response force is likely to successfully interdict this type of attack. Prob(0.6 to 0.8)
- ○ c. Facility security response force is almost equally likely to succeed or fail in interdicting this type of attack. Prob(0.4 to 0.6)
- ○ d. Facility security response force is unlikely to successfully interdict this type of attack. Prob(0.2 to 0.4)
- ○ e. Facility security response force is extremely unlikely to successfully interdict this type of attack. Prob(0 to 0.2)

Facility security response force capability assumptions:
[Q:7.22-7411, Q:8.22-9614, Q:10.22-9772, Q:12.22-7662, Q:13.22-9953]

Offsite Security Response Force Capability

This refers to the probability that an offsite security response force (if any) is able to interdict an adversary force before it is successful in executing an attack (assuming the onsite force failed).

The likelihood of success of an offsite response force may be low unless the facility has coordinated with local law enforcement and integrated them into facility planning (including exercises). Also, the staffing, training, and equipment of the response force for the type of attack should be considered before credit is given for response force effectiveness in interdicting an attack.

How likely is the designated offsite security response force (such as local law enforcement personnel) to successfully interdict the adversary force before they are successful in executing their attack (given that the onsite team failed)?
[Q:7.22-7412, Q:8.22-9615, Q:10.22-9773, Q:12.22-7663, Q:13.22-9954]

- ○ a. Offsite security response force is almost certain to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.8 to 1.0)
- ○ b. Offsite security response force is likely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.6 to 0.8)
- ○ c. Offsite security response force is almost equally likely to succeed or fail in interdicting this type of attack, assuming that the facility force was not successful. Prob(0.4 to 0.6)
- ○ d. Offsite security response force is unlikely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.2 to 0.4)
- ○ e. Offsite security response force is extremely unlikely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0 to 0.2)

Offsite security response force capability assumptions:
[Q:7.22-7413, Q:8.22-9616, Q:10.22-9774, Q:12.22-7664, Q:13.22-9955]

Achievability Probability

This refers to the probability that an adversary could execute a successful attack assuming the absence of all security measures. Achievability is a function of the difficulty for the adversary to attack the specific target asset.

Factors which may contribute to an achievability probability less than 1.0 could include:

- Inaccuracy of a standoff weapon
- Difficulty in attacking a point target with the specified aircraft (particularly if the asset is in among many other pieces of equipment or units)
- Difficulty in loading a large but portable package
- Difficulty in effectively contaminating a COI shipment

How likely is the adversary to succeed in accomplishing this attack (giving no credit for any facility or asset security measures)?
[Q:7.22-7414, Q:8.22-9617, Q:9.22-9689, Q:10.22-9775, Q:11.22-9904, Q:12.22-7665, Q:13.22-9956]

- ○ a. Adversary is extremely unlikely achieve success with this attack even if security measures are not implemented. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to achieve success with this attack even if security measures are not implemented. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in this attack if security measures are not implemented. Prob(0.4 to 0.6)
- ○ d. Adversary is likely to achieve success with this attack assuming security measures are not implemented. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to achieve success with this attack assuming security measures are not implemented. Prob(0.8 to 1.0)

Achievability assumptions:
[Q:7.22-7415, Q:8.22-9618, Q:9.22-9690, Q:10.22-9776, Q:11.22-9905, Q:12.22-7666, Q:13.22-9957]

Target Hardness Probability

This refers to the probability that an adversary that reached a target and executed the attack did not damage the asset sufficiently to cause the intended COI release event onsite or successfully steal/divert the COI for use in an attack.

Do not give additional credit for considerations you have already credited in evaluation of earlier factors (e.g., achievability, identifiability). This factor represents the inherent hardness or location of the target that protects it from the effects of an attack that was successfully initiated. Examples of situations where credit could be assessed include:

- Tanks located in a manner (e.g., underground or mounded) where an explosive device located at the closest point available would not necessarily cause its catastrophic failure
- A vessel with multiple layers or insulation that provides spacing such that a standoff weapon would not be effective in penetrating the vessel

What is the probability that the asset would withstand the attack (i.e., suffers less than a catastrophic release/explosion or loss of COI to theft/diversion), assuming that the adversary is successful at accessing the target and executing the specific type of attack?
[Q:7.22-7416, Q:8.22-9619, Q:10.22-9777, Q:11.22-9906, Q:13.22-9958]

- ○ a. The target is very hard against/resistant to this kind of attack, it is almost certain that this type of attack will not create a catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.8 to 1.0)
- ○ b. The target is relatively hardened against/resistant to this type of attack, it is likely that this type of attack will not create a catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.6 to 0.8)
- ○ c. The target is equally likely to withstand to this type of attack or to fail (resulting in a catastrophic release, explosion, or loss of COI to theft/diversion). Prob(0.4 to 0.6)
- ○ d. The target is not very resistant to this type of attack and is unlikely to survive this type of attack without catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.2 to 0.4)
- ○ e. The target is not resistant to this type of attack, and is extremely unlikely to survive this type of attack without catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0 to 0.2)

Target hardness assumptions:
[Q:7.22-7417, Q:8.22-9619, Q:10.22-9778, Q:11.22-9907, Q:13.22-9959]

Availability Probability

This factor accounts for situations where the asset (or group of assets) only contains the applicable COI for a limited amount of time, on a schedule not readily available to the adversary. For example, select "a" for a batch process tank that only contains the COI for one hour every 24 hours, on a schedule not available or visible to the adversary.

How likely is the specific asset attacked to contain the relevant COI, assuming that the adversary identifies and attacks the correct target asset?
[Q:7.22-8911, Q:8.22-9624, Q:9.22-9694, Q:10.22-9782, Q:11.22-9911, Q:12.22-9361, Q:13.22-9961]

- ○ a. Attack is extremely unlikely to occur at a time the asset contains a significant quantity of the COI. Prob(0 to 0.2)
- ○ b. Attack is unlikely to occur at a time the asset contains a significant quantity of the COI. Prob(0.2 to 0.4)
- ○ c. Attack is equally likely to occur at a time the asset contains or does not contain a significant quantity of the COI. Prob(0.4 to 0.6)
- ○ d. Attack is likely to occur at a time the asset contains a significant quantity of the COI. Prob(0.6 to 0.8)
- ○ e. Attack is almost certain to occur at a time the asset contains a significant quantity of the COI. Prob(0.8 to 1.0)

Availability assumptions:
[Q:7.22-8912, Q:8.22-9625, Q:9.22-9695, Q:10.22-9783, Q:11.22-9912, Q:12.22-9362, Q:13.22-9962]

Unauthorized Customer Registration

This refers to the probability that an adversary can register himself/herself as a customer for purchase of the COI.

This vulnerability assesses the probability of success or failure of the facility's customer validation procedures. For example, many customer validation programs verify (1) customers' end-use for the COI, (2) integrity of the customers' business operations, (3) the customers' ability to pay and method of payment, and (4) the customers' packaging and shipping requirements. Another aspect of this vulnerability is the strength (or weakness) in the facility's cyber business system that maintains the approved customer list such that it prevents (or allows) the adversary to establish itself as an approved customer.

How likely is the adversary to be able to register as a new customer that is approved to purchase theft/diversion COI?
[Q:12.8-7682]

- ○ a. Adversary is extremely unlikely to successfully register as a new client to purchase the specific COI involved in this scenario. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to successfully register as a new client to purchase the COI involved in this scenario. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in registering as a new client approved to purchase COI involved in this scenario. Prob(0.4 to 0.6)
- ○ d. Adversary is likely to succeed in registering as a new client approved to purchase COI. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to successfully register as a new client authorized to purchase COI. Prob(0.8 to 1.0)

Unauthorized customer registration assumptions:
[Q:12.8-7683]

Unauthorized Order Placement

This vulnerability factor assumes the adversary (who is not an authorized customer) is misusing an established customer's account and can place an order for shipment to his/her chosen location. This factor is designed to assess an individual's (adversary) ability to defeat the facility's (or company's) procedures for identifying, validating and vetting a customer seeking to purchase and receive delivery of a COI. For example, certain COI are prohibited from pick up and always delivered directly to a customer by the facility. Other companies only ship to pre-determined and approved locations. This factor aims to assess the reliability of the facility's (or company's) order processing procedures.

How likely is the adversary to be able to place an order for this COI for an authorized customer that would allow shipment to a location where the adversary could accept the shipment?
[Q:12.8-7684]

- ○ a. Adversary is extremely unlikely to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in placing an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.4 to 0.6)
- ○ d. Adversary is likely to succeed in placing an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.8 to 1.0)

Unauthorized order placement assumptions:
[Q:12.8-7685]

Unauthorized Order Pickup

If the answer to "Is the customer permitted to pick up orders at this asset?" [Q:12.6-7736] is No, skip Unauthorized Order Pickup.

This refers to the probability that an adversary could pick up an order being held for an authorized customer.

This vulnerability assumes that the adversary has not been able to place an order. The ability of the adversary to pick up an authorized customer's order could result, for example, from a facility's failure to secure its shipping and receiving. Another possible factor in this assessment is the trustworthiness of the facility's personnel involved in the physical packing, staging and shipping processes.

How likely is the adversary to be able to pick up an order for an authorized customer for this COI?
[Q:12.8-7686]

- ○ a. Adversary is extremely unlikely to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0 to 0.2)
- ○ b. Adversary is unlikely to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0.2 to 0.4)
- ○ c. Adversary is equally likely to succeed or fail in picking up an order that is intended for pickup by an authorized customer. Prob(0.4 to 0.6)
- ○ d. Adversary is likely to succeed in picking up an order that is intended for pickup by an authorized customer. Prob(0.6 to 0.8)
- ○ e. Adversary is almost certain to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0.8 to 1.0)

Unauthorized order pickup assumptions:
[Q:12.8-7687]

Computer Systems Analysis

Are personnel allowed to carry portable cyber equipment into the facility (e.g., laptop computers, personal digital assistants (PDAs), flash drives, data disks, and smart cell phones)?
[Q:14.09-4151]

- ○ Yes
- ○ No

Are personnel screened at facility entrances for unauthorized cyber related equipment?
[Q:14.09-4152]

- ○ Yes
- ○ No

If No, skip the next question.

Has the personnel screening process been validated through testing by professional security services?
[Q:14.091-4153]

- ○ Yes
- ○ No

The following pages should be answered for each cyber control system and cyber business system you have listed.

Copy the following pages (100 - 107) relating to cyber control and cyber business systems and answer the questions for each system listed above Enter each control system (cyber control or cyber business) listed on page 67 or 68, and answer the following questions pertaining to that system. Each system must be answered separately.

Cyber Name

If the control system is cyber control, skip the next two questions.

Is this cyber system physically located at the facility?
[Q:14.61-4175]

- ○ Yes
- ○ No

If No, please provide the address of the cyber business system.
If Yes, the application will require the user to identify the location of the cyber business system on a map of the facility.

Enter the cyber system location.

Enter the Country
[Q:14.62-8232]

Location/Building Name
[Q:14.63-4177]

Street
[Q:14.63-4178]

Street Line 2
[Q:14.63-8271]

City
[Q:14.63-4179]

Province or State
[Q:14.63-4180, Q:14.63-8233]

ZIP Code
[Q:14.63-4181]

Cyber System Map

Provide a map that identifies the location of the cyber control system.
If the answer to [Q:14.61-4175] "Is this cyber system physically located at the facility?" is Yes, provide a map that identifies the location of the cyber business system.

Control System Analysis

Is external access (e.g., Internet, modem, wireless) to cyber systems allowed?
[Q:14.3-1614, Q:14.8-1033]

- ○ Yes
- ○ No

If No, skip the next question.

Has the lack of external access been validated through testing by IT security professional services?
[Q:14.31-1633, Q:14.81-1034]

- ○ Yes
- ○ No

Are the capabilities of the cyber systems in the facility limited in regard to communications with portable cyber equipment (authorized or not) (e.g. laptop computers, personal digital assistants (PDAs), flash drives, data disks, smart cell phones)?
[Q:14.32-1635, Q:14.82-1035]

- ○ Yes
- ○ No

If Yes, skip the next question.

Has the disabling of communication capabilities been validated through testing by a professional IT security service?
[Q:14.33-1637, Q:14.83-1036]

- ○ Yes
- ○ No

Security Policy

Does the facility have documented and distributed cyber security policies, plans and supporting procedures commensurate with the current information technology operating environment?
[Q:14.34-1692, Q:14.84-1051]

- ○ Policies, plans, and procedures
- ○ (Policies or plans) and procedures
- ○ (Policies and/or plans) but no procedures
- ○ Procedures only
- ○ Any of the above, but not distributed
- ○ Not at all

Does the facility have a documented and distributed cyber change management policy and supporting procedures (e.g., new hardware/software, employee access)?
[Q:14.34-1693, Q:14.84-1071]

- ○ Policies and procedures
- ○ Policies or procedures
- ○ Either of the above, but not distributed
- ○ Not at all

Has an individual(s) been designated as responsible for cyber security at the facility?
[Q:14.34-1694, Q:14.84-1072]

- ○ Yes
- ○ Informal
- ○ No

Cyber Access Control

Does the facility allow systems to have external connections with portable electronic devices configured for minimum business needs and verified with scans?
[Q:14.34-2851, Q:14.84-2811]

- ○ External connections with or without portable electronic devices, and/or not configured for minimum business needs, and/or not verified with scans
- ○ No external connections, no portable electronic devices allowed, systems block external devices and media, and verified with scans
- ○ External connections are configured for minimum business needs and verified with scans, no portable electronic devices allowed, systems block external devices and media, and verified with scans
- ○ External connections with portable electronic devices allowed - configured for minimum business needs and verified with scans
- ○ Other

Does the facility practice the concept of least privilege (e.g., users are only granted access to those files and applications based on roles and responsibilities)?
[Q:14.34-1695, Q:14.84-1092]

- ○ Yes
- ○ Users of critical processes or systems
- ○ No

Have all default passwords been changed to user-specific passwords?
[Q:14.34-1696, Q:14.84-1093]

- ○ Yes
- ○ Partial or critical systems
- ○ No

Are accounts locked out after several unsuccessful login attempts?
[Q:14.34-1697, Q:14.84-1094]

- ○ 3 or fewer attempts
- ○ 4 – 5 attempts
- ○ > 5 attempts
- ○ Not at all

Personnel Security

Does the facility perform background checks for personnel in critical/sensitive positions?
[Q:14.35-1719, Q:14.85-1100]

- ○ Employees and contractors on a periodic basis
- ○ Employees only on a periodic basis
- ○ Employees and contractors on a one-time basis
- ○ Employees only on a one-time basis
- ○ Not at all

Does the facility actively maintain the access control list to ensure that all cyber system accounts are modified, deleted, or de-activated as personnel leave the company or transfer into new roles?
[Q:14.35-1720, Q:14.85-1101]

- ○ Immediately
- ○ Before close of business
- ○ Within one week
- ○ Not at all

Physical and Environmental

Does the facility restrict physical access to sensitive or restricted IT, telecommunications, media storage and control areas to those with appropriate need?
[Q:14.35-1721, Q:14.85-1105]

- ○ Yes
- ○ Not at all
- ○ No

Awareness and Training

Does the facility provide cyber security training?
[Q:14.35-1723, Q:14.85-1107]

- ○ Prior to system access
- ○ Within first week
- ○ Within first month
- ○ Not at all

Monitoring and Incident Response

Does the facility log cyber security events on systems and review them on a regular basis?
[Q:14.36-1727, Q:14.86-1151]

- ○ Yes – review by automated means
- ○ Yes – reviewed at least weekly
- ○ Yes – review manually at least monthly
- ○ Some degree of logging with some degree of review
- ○ Not at all

Does the facility log cyber security events on servers, and review them on a regular basis?
[Q:14.36-2852, Q:14.86-2831]

- ○ Yes – review by automated means
- ○ Yes – reviewed at least weekly
- ○ Yes – review manually at least monthly
- ○ Some degree of logging with some degree of review
- ○ Not at all

Does the facility report significant cyber security events to senior management?
[Q:14.36-1728, Q:14.86-1152]

- ○ Yes
- ○ Sometimes
- ○ No

Does the facility mandate malicious code protection on all systems?
[Q:14.36-1730, Q:14.86-1153]

- ○ Not at all, or not DAT file updates
- ○ Yes
- ○ No

Does the cyber system allow email?
[Q:14.37-1735, Q:14.87-1173]

- ○ Yes
- ○ No

If No, skip the next question.

Are email attachments (e.g., executable files) filtered on incoming email?
[Q:14.38-1737, Q:14.88-1174]

- ○ Not at all, or not DAT file updates
- ○ Yes
- ○ No

If the control system is business related, skip the next two questions.

Are there Safety Instrumented Systems (SIS) or other watch-dog systems, independent of the systems they monitor, that provide interlocks or response to prevent or mitigate catastrophic events and/or the consequences of a cyber attack?
[Q:14.39-1175]

- ○ Yes – with external connections
- ○ Yes – not networked with their control systems and no external connections
- ○ Yes – but networked with their control systems – no other external connections
- ○ Yes – with external connections
- ○ No

If Yes, skip the next question.

Has the facility disabled all modems or other external access connections to these systems?
[Q:14.391-1176]

- ○ Yes
- ○ No

Configuration Management

Has a business requirement been established for every external connection into the network/environment, including wireless and modem connections?
[Q:14.4-1741, Q:14.9-1191]

- ○ Yes
- ○ Partial
- ○ No

Does the facility apply/perform regular software and hardware, patches, updates, upgrades, and replacements?
[Q:14.4-1742, Q:14.9-1192]

- ○ Dynamic
- ○ As available
- ○ Monthly
- ○ More than once a month
- ○ Not at all

Are configuration changes to the network and application's hardware and software reviewed by an IT security professional and by management to assess the security impact prior to the changes being implemented to the operational environment?
[Q:14.4-1743, Q:14.9-1193]

- ○ IT security and management review for network and applications
- ○ IT security or management review for network and applications
- ○ Partial
- ○ Not at all

Risk and Vulnerability Management

Have potential vulnerabilities of critical assets, systems, and networks been identified and evaluated?
[Q:14.4-2854, Q:14.9-2832]

- ○ Partial or not at all
- ○ Identified and evaluated
- ○ Identified but not evaluated

Does the facility have a means to identify and measure cyber security risk (including requirements, processes, and procedures) that is based on recognized cyber security methodologies, standards, or best practices?
[Q:14.4-1744, Q:14.9-1195]

- ○ Yes
- ○ Partial
- ○ No

Are network and system (application) level security tests performed (vulnerability scans, penetration tests, open communication line scans, authorized hardware and software scans) on a regular basis; and after configuration changes or being patched or upgraded - before being put into operation?
[Q:14.4-2855, Q:14.9-2833]

- ○ Partial or not at all
- ○ Network and applications monthly or more often; and after all configuration changes, patches, and upgrades
- ○ Network and applications quarterly or longer; and after all configuration changes, patches, and upgrades
- ○ Network and applications after all configuration changes, patches, and upgrades, but not on a regularly scheduled basis
- ○ Network and applications monthly or more often
- ○ Network and applications quarterly or longer

Has the facility incorporated the vulnerability solutions that are applicable and appropriate for the environment (e.g., are firewalls configured for minimum business or operational needs)?
[Q:14.4-2856, Q:14.9-2834]

- ○ Incorporated all appropriate historic and current solutions
- ○ Partial
- ○ Not at all