CSAT Site Security Plan

Questions

June 2011

Version 2.0

Homeland Security

Table of Contents

General 1
Facility Information 3
Risk-based Performance Standards 55
Completion 59
Finish 59
RBPS 1 – Restrict Area Perimeter 61
RBPS 2 – Secure Site Assets 85
RBPS 3 – Screening and Access Control 113
RBPS 4 – Detect, Deter, and Delay 137
RBPS 5 – Shipping, Receiving, and Storage 161
RBPS 6 – Theft and Diversion 177
RBPS 7 – Sabotage 187
RBPS 8 – Cyber Security 199
RBPS 9 – Response 219
RBPS 10 – Monitoring 235
RBPS 11 – Training 243
RBPS 12 – Personnel Surety 255
RBPS 13 – Elevated Threats 263
RBPS 14 – Specific Threats 269
RBPS 15 – Reporting Significant Security Incidents 273
RBPS 16 – Investigating Significant Security Incidents 281
RBPS 17 – Officials and Organization 287
RBPS 18 – Records 293

This page intentionally left blank.

General

- **Please be sure you are familiar with the CFATS Regulation, the RBPS Guidance, and the SSP Instruction Manual before using the SSP tool.**
- **The CSAT SSP tool collects information from covered facilities regarding existing and if a covered facility so chooses - planned and proposed security measures. Facilities are required to list and/or describe existing security measures as part of their CSAT SSP submissions. However, this SSP tool will provide facilities the opportunity to propose that certain existing and/or planned security measures identified in this tool not be considered by DHS in evaluating their SSPs for approval. Of course, if a facility chooses not to provide information about an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.**
- **Paperwork Burden Disclosure Notice:**
  The public reporting burden for this form is estimated to be 200 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 Site Security Plan 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 SSP) unless a valid OMB control number is displayed. NOTE: DO NOT send the completed CSAT SSP to the above address.
- **Even if your facility is uploading an ASP, the facility is still directed to answer all questions related to the General Section of the SSP tool and the Facility Operations Section of the SSP tool before uploading your ASP.**
- **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).

This page intentionally left blank.

Facility Information

Facility Address

Facility Name
Provide the name of the facility. The name must be specific to the facility; if the facility is part of a large corporation, the name may be the corporate name plus the location (for example, 'ABC Oil/Refining - Hightown Plant').

Alternate Facility Name
Provide alternative names under which the facility may be known.

Street Address
Enter the street address of the facility's physical location. [Note: This may be different from the mailing address.] Use local street and road designations, not post office or rural box numbers.

Street Address (continued)

Street Address (continued)

City
Enter the city of the facility's physical location. [Note: This may be different from the mailing address.]

State

ZIP Code
Enter the ZIP Code (including the 4 digit extension, if applicable) of the facility's physical location. For example, XXXXX or XXXXX-XXXX are valid ZIP Code formats. [Note: This may be different from the mailing address.]

County
Provide additional county names in which this facility is located.

DHS Final Notification Letter

This section asks several questions to verify the content of the facility's DHS Final Notification Letter. Any differences between the DHS Final Notification Letter content and the prepopulated information that appears below must be reported to the help desk before continuing with the SSP Tool.

Please refer to your Facility's DHS Final Notification Letter when completing this section.

Is the prepopulated information listed above consistent with the information found on the facility's DHS Final Notification Letter? [Q:1.9-13848]

- ○ Yes
- ○ No

Security/Vulnerability Issues Related to Other COI of Concern to the Facility

In addition to the information identified in the facility's DHS Final Notification Letter, this section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

If the facility answers Yes to a security/vulnerability issue, the associated COI list will reflect the information from the facility's Final Notification letter. The facility may then enter any additional COI of concern.

Does the facility have security/vulnerability issues related to release-toxic COI? [Q:2.0-13720]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to release-flammable COI? [Q:2.0-13722]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to release-explosive COI? [Q:2.0-13724]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to theft-EXP/IEDP COI? [Q:2.0-13726]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to theft-WME COI? [Q:2.0-13728]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to theft-CW/CWP COI? [Q:2.0-13730]

- ○ Yes
- ○ No

Does the facility have security/vulnerability issues related to sabotage/contamination COI? [Q:2.0-13732]

- ○ Yes
- ○ No

Release Toxic Chemicals of Interest

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following release toxic chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.1-13765] **Check all that apply.**

Chemical Name	CAS#	Yes	No
Acrolein [2-Propenal or Acrylaldehyde]	107-02-8	○	○
Allyl alcohol [2-Propen-1-ol]	107-18-6	○	○

Chemical Name	CAS#	Yes	No
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, (ClO2)]	10049-04-4	○	○
Chloroform [Methane, trichloro-]	67-66-3	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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 oxychlorid [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 (SF4), (T-4)-]	7783-60-0	○	○

Chemical Name	CAS#	Yes	No
Sulfur trioxide	7446-11-9	○	○
Tetramethyllead [Plumbane, tetramethyl-]	75-74-1	○	○
Titanium tetrachloride [Titanium chloride (TiCl4) (T-4)-]	7550-45-0	○	○

Release Flammable Chemicals of Interest

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following release flammable chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.2-13766] **Check all that apply.**

Chemical Name	CAS#	Yes	No
Acetaldehyde	75-07-0	○	○
Acetylene [Ethyne]	74-86-2	○	○
Acrylonitrile [2-Propenenitrile]	107-13-1	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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-]	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	○	○
Ethyl ether [Ethane, 1,1-oxybis-]	60-29-7	○	○
Ethyl mercaptan [Ethanethiol]	75-08-1	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
1-Pentene	109-67-1	○	○
2-Pentene, (E)-	646-04-8	○	○
2-Pentene, (Z)-	627-20-3	○	○
Peracetic acid [Ethaneperoxic acid]	79-21-0	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
Vinyl acetate monomer [Acetic acid ethenyl ester]	108-05-4	○	○
Vinyl acetylene [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

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following release explosive chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.3-13767] **Check all that apply.**

Chemical Name	CAS#	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	○	○
HMX [Cyclotetramethylene-tetranitramine]	2691-41-0	○	○
Lead azide	13424-46-9	○	○
Lead styphnate [Lead trinitroresorcinate]	15245-44-0	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following theft/diversion EXP/IEDP chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.4-13768] **Check all that apply.**

Chemical Name	CAS#	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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
Nitrotriazolone	932-64-9	○	○
Octolite	57607-37-1	○	○
Octonal	78413-87-3	○	○
Pentolite	8066-33-9	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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 Weapon of Mass Effect (WME) Chemicals of Interest

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following theft/diversion WME chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.5-13769] **Check all that apply.**

Chemical Name	CAS#	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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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 (SF4), (T-4)-]	7783-60-0	○	○
Tellurium hexafluoride	7783-80-4	○	○
Titanium tetrachloride [Titanium chloride (TiCl4) (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

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following theft/diversion CW/CWP chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.6-13770] **Check all that apply.**

Chemical Name	CAS#	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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
VX [o-Ethyl-S-2-diisopropylaminoethyl methyl phosphonothiolate]	50782-69-9	○	○

Sabotage/Contamination Chemicals of Interest

This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues and COI of concern.

Which of the following sabotage/contamination chemicals of interest (COI) raise security/vulnerability issue(s) for the facility? [Q:2.7-13771] **Check all that apply**.

Chemical Name	CAS#	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	○	○

Chemical Name	CAS#	Yes	No
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, (ClO2)]	10049-04-4	○	○
Chloroacetyl chloride	79-04-9	○	○
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	○	○

Chemical Name	CAS#	Yes	No
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	○	○
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	○	○

Chemical Name	CAS#	Yes	No
Sodium phosphide	12058-85-4	○	○
Strontium phosphide	12504-16-4	○	○
Sulfuryl chloride	7791-25-5	○	○
Thionyl chloride	7719-09-7	○	○
Titanium tetrachloride [Titanium chloride (TiCl4) (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	○	○

CSAT Submissions

Is this the initial CSAT SSP Submittal? [Q:2.94-18411]

○ Yes

○ No

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

Most Recent CSAT Top Screen
On what date did the facility submit its most recent CSAT Top Screen? [Q:2.95-18409]

Most Recent CSAT SVA
On what date did the facility submit its most recent CSAT SVA? [Q:2.95-18410]

If this is not the initial CSAT SSP Submittal, go to Facility Description.

Most Recent CSAT SSP
On what date did the facility submit its most recent CSAT SSP? [Q:2.95-18412]

Facility Description

Choose the facility type that best describes your facility.

What is the facility type? [Q:3.0-13871] (Choose one: Agricultural Chemicals Distribution, Agricultural Chemicals Manufacturing, Agricultural Products Processing, Chemical Distribution, Chemical Manufacturing, College/University, Food Distribution, Food Processing, Health Care, Mineral Extraction/Processing, Natural Gas Storage/Transfer, Petroleum Products Distribution, Petroleum Refining, Pharmaceutical Manufacturing, Power Generation, Propane Distribution, Research, Waste Management, Other)

If "Other" is selected, enter a description: [Q:3.0-14051]

Provide the Office of Emergency Management (OEM) authority under which the facility operates.

What is the Office of Emergency Management (OEM) authority? [Q:3.0-13934] (Choose one: County, Township, City, Village, Borough, Other)

If "Other" is selected, enter a description: [Q:3.0-14052]

Enter the name of the local jurisdiction: [Q:3.0-13935]

Choose the locale setting that best describes the facility.
What is the locale setting of the facility? [Q:3.0-13936] (Choose one: Inside a city or town, In an industrial park or zone, In a suburb or residential area, In a rural setting, Other)

If "Other" is selected, enter a description: [Q:3.0-13937]

Choose the construction that best describes the facility.

What is the construction type of the facility? [Q:3.0-14053] (Choose one: Inside a building or buildings, Outdoor process equipment, Both inside a building and outdoor process equipment, Other)

If "Other" is selected, enter a description: [Q:3.0-14054]

Facility Contact Information

Facility Security Officer

Name of the facility security officer: [Q:3.1-13939]

Phone number of the security officer: [Q:3.1-13940]

Assistant Facility Security Officer

Name of the assistant facility security officer: [Q:3.1-13941]

Phone number of the assistant security officer: [Q:3.1-13942]

Corporate Security Officer

Name of the corporate security officer: [Q:3.1-13943]

Phone number of the corporate security officer: [Q:3.1-13944]

Cyber Security Officer

Name of the cyber security officer: [Q:3.1-13945]

Phone number of the cyber security officer: [Q:3.1-13946]

Does the facility implement security plans required or recommended by the following agencies? [Q:3.1-18675]

Agency	Yes	No
TSA	○	○
DOT	○	○
Coast Guard	○	○
Customs	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:3.1-18676]

On-site Emergency Response Capabilities

Does the facility have a fire department? [Q:3.9-18433]

○ Yes
○ No

Does the facility have a HAZMAT team? [Q:3.9-18434]

- ○ Yes
- ○ No

Does the facility share any of its emergency response capabilities with other facilities or entities? [Q:3.9-18435]

- ○ Yes
- ○ No

If "No" is selected, go to question [Q:3.9-18436].

On-site Emergency Response Capability Sharing Entities

Identify the other facilities or entities with which this facility shares emergency response capabilities.

Other Facility or Entity Sharing Emergency Response Capability [Q:3.91-18442]

Does the facility have an emergency management team available? [Q:3.9-18436]

- ○ Yes
- ○ No

If "No" is selected, go to question [Q:3.9-18437].

On-site Emergency Management Team

Enter the number of on-site emergency management team members [Q:3.91-18444]

Does the facility have any Special Response Capabilities? [Q:3.9-18437]

- ○ Yes
- ○ No

If "No" is selected, go to Emergency Management Information.

Choose the special response capability available on-site. Select all capabilities that apply. [Q:3.91-18445]

On-site Special Response Capability	Yes	No
Armored Vehicle	○	○
Aviation	○	○
Bomb Response	○	○
CBRNE Response	○	○
Disaster Support Services	○	○
Emergency Medial	○	○
Explosion Response	○	○
Field Medical	○	○
Fire Response	○	○
Hostage Rescue	○	○
Maritime	○	○
Mass Casualty Management	○	○
Negotiator	○	○
Police Investigatory	○	○
Snipers	○	○
Tactical (Combat)	○	○
Tactical (Command & Control)	○	○
Toxic Release Response	○	○

Emergency Management Information

Is the facility able to shelter-in-place? [Q:4.0-18738]

○ Yes
○ No

Does the facility have a community notification system? [Q:4.0-18749]

○ Yes
○ No

Local Police Jurisdiction

Name of the local police jurisdiction: [Q:4.0-13949]

Phone number of the cyber security officer: [Q:4.0-13950]

Local Police Capability

Number of full-time police officers: [Q:4.0-13951]

Local police SWAT team available? [Q:4.0-13952]

- ○ Yes
- ○ No
- ○ Unknown

Local police bomb squad available? [Q:4.0-13953]

- ○ Yes
- ○ No
- ○ Unknown

Local police HAZMAT team available? [Q:4.0-13954]

- ○ Yes
- ○ No
- ○ Unknown

Local police Emergency Management Capabilities available? [Q:4.0-17899]

- ○ Yes
- ○ No
- ○ Unknown

Local Police Response

Round distance up to nearest tenth of a mile. (For example, for 0.25 miles enter 0.3 miles)

Distance to nearest police station (miles): [Q:4.0-13955]

Time for first response officer to reach facility (average): [Q:4.0-13957] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Minimum time needed for police to mount tactical response: [Q:4.0-13959] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Was the tactical response time tested? [Q:4.0-13960]

- ○ Yes
- ○ No

If "No" is selected, go to question [Q:4.0-18750.

Date of tactical response test: [Q:4.0-13961]

Does the police department conduct response tests outside of a facility drill or exercise? [Q:4.0-18750]

- ○ Yes
- ○ No
- ○ Unknown

On-site Fire Fighting Capability

Number of full-time on site fire fighters: [Q:4.1-19181]

On-site fire dept. foam truck available? [Q:4.1-19182]

- ○ Yes
- ○ No
- ○ Unknown

On-site fire dept. HAZMAT team available? [Q:4.1-19183]

- ○ Yes
- ○ No
- ○ Unknown

On-site fire dept. EMT available? [Q:4.1-19184]

- ○ Yes
- ○ No
- ○ Unknown

Local Fire Jurisdiction

Name of the local fire jurisdiction: [Q:4.1-13968]

Phone number of the local fire department: [Q:4.1-13969]

Local Fire Fighting Capability

Number of full-time fire officers: [Q:4.1-13970]

Local fire dept. foam truck available? [Q:4.1-13972]

- ○ Yes
- ○ No
- ○ Unknown

Local fire dept. HAZMAT team available? [Q:4.1-13973]

- ○ Yes
- ○ No
- ○ Unknown

Local fire department EMT available? [Q:4.1-13971]

- ○ Yes
- ○ No
- ○ Unknown

Local Fire Fighting Response

Round distance up to nearest tenth of a mile. (For example, for 0.25 miles enter 0.3 miles)

Distance to nearest fire dept. station (miles): [Q:4.1-13974]

Time for first response apparatus to reach facility (average): [Q:4.1-13975] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Minimum time needed for fire department to set up and respond once on-site at the facility: [Q:4.1-13976] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Was the response time tested? [Q:4.1-13977]

- ○ Yes
- ○ No

If "No" is selected, go to question [Q:4.2-19185].

Date of response test: [Q:4.1-13978]

On-site EMT Capability

Number of full-time EMT officers: [Q:4.2-19185]

On-site EMT life support unit available? [Q:4.2-19186]

- ○ Yes
- ○ No
- ○ Unknown

On-site EMT water rescue available? [Q:4.2-19187]

- ○ Yes
- ○ No
- ○ Unknown

On-site EMT HAZMAT team available? [Q:4.2-19188]

- ○ Yes
- ○ No
- ○ Unknown

Local EMT Jurisdiction

Name of the EMT jurisdiction: [Q:4.2-13979]

Phone number of the local EMT [Q:4.2-13980]

Local EMT Capability

Number of full-time EMT staff: [Q:4.2-13981]

Local EMT life support unit available? [Q:4.2-13982]

- ○ Yes
- ○ No
- ○ Unknown

Local EMT water rescue available? [Q:4.2-13983]

- ○ Yes
- ○ No
- ○ Unknown

Local EMT HAZMAT team available? [Q:4.2-13984]

- ○ Yes
- ○ No
- ○ Unknown

Local EMT Response

Round distance up to nearest tenth of a mile. (For example, for 0.25 miles enter 0.3 miles)

Distance to nearest Trauma Center (miles): [Q:4.2-13985]

Time for first response EMT to reach facility (average): [Q:4.2-13986] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Minimum time needed to transport casualties to Trauma Center: [Q:4.2-13987] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Was the response time tested? [Q:4.2-13988]

- ○ Yes
- ○ No

If "No" is selected, go to question [Q:4.2-13989].

Date of response test: [Q:4.2-13989]

Local Mutual Assistance Group (MAG)

List all of the Local Mutual Assistance Groups (MAG), if any, associated with the facility. [Q:4.3-17712]

For each listed MAG, answer the related questions (page 37).
When finished listing all of the MAG, go to Special Response Capability (page 38).

Local Mutual Assistance Group (MAG)

Short description of the local mutual assistance group: [Q:4.31-13990]

Phone number of the local MAG: [Q:4.31-13991]

How many groups/facilities are included in the MAG? [Q:4.31-18839]

Local MAG Capability
Number of MAG member companies: [Q:4.31-13994]

Local MAG Response

Time for capable response to reach facility (average): [Q:4.31-13999] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Does the facility conduct drills or exercises to include the MAG? [Q:4.31-18840]

- ○ Yes
- ○ No

Minimum time needed for MAG to begin on-scene response: [Q:4.31-14000] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Was the response time tested? [Q:4.31-14001]

- ○ Yes
- ○ No

If "No" is selected, skip the next question.

Date of response test: [Q:4.31-14002]

Special Response Capability

Response Agencies with Other Special Capabilities
Are other special response capabilities available? [Q:4.4-14030]

- ○ Yes
- ○ No
- ○ Unknown

If "No" is selected, go to Facility Personnel (page 41).

If capabilities exist for an agency that is not listed, indicate the additional capabilities below and describe them. Use the blank spaces provide to add any additional capabilities not listed.

Responding Agency [Q:4.4-14031], [Q:4.5-14038]	**Yes**	**No**
FBI	○	○
ICE	○	○
TSA	○	○

Responding Agency [Q:4.4-14031], [Q:4.5-14038]	**Yes**	**No**
US Army Bomb Squad	○	○
US Army CBRNE Team	○	○
US Coast Guard	○	○
US Marine Corps CBRNE Team	○	○
US Marshals or other Fed Law Enforcement	○	○
CDC	○	○
EPA	○	○
FDA	○	○
State Police	○	○
State Environmental Agency	○	○
Office of Emergency Management	○	○
County Police	○	○
County HAZMAT	○	○
Sheriff	○	○
Bomb Squad	○	○
Maritime Law Enforcement	○	○
American Red Cross	○	○
Salvation Army	○	○

Responding Agency
For each Responding Agency selected in [Q:4.4-14031], [Q:4.5-14038], *enter the name and answer the capability questions below.*

Choose the government level providing the special capability.
What is the government level? [Q:4.41-14056], [Q:4.51-14062] (Choose one: Federal (DHS), Federal (DOJ), State, County, Municipal, Township, Local, NGO, Other).

If "Other" is selected, enter a description: [Q:4.41-14067], [Q:4.51-14069]

What is the distance from the responding agency (miles)? [Q:4.41-14057], [Q:4.51-14063]

What is the average arrival time for the response? [Q:4.41-14058], [Q:4.51-14064] (Choose one: 1 minute, 2 minutes, 3 minutes…60 minutes, unknown).

Is there a formal, written agreement with the responding agency? [Q:4.41-14060], [Q:4.51-14066]

- ○ Yes
- ○ No

Choose the special response capability. Select all capabilities that apply.

Special Response Capability [Q:4.41-14059], [Q:4.51-14065]	**Yes**	**No**
Armored Vehicle	○	○
Aviation	○	○
Bomb Response	○	○
CBNE Response	○	○
Disaster Support Services	○	○
Emergency Medical	○	○
Explosive Response	○	○
Field Medical	○	○
Fire Response	○	○
Hostage Rescue	○	○
Maritime	○	○
Mass Casualty Management	○	○
Negotiator	○	○
Police Investigatory	○	○
Snipers	○	○

Special Response Capability [Q:4.41-14059], [Q:4.51-14065]	**Yes**	**No**
Tactical (Combat)	○	○
Tactical (Command & Control)	○	○
Toxic Release Response	○	○

Facility Personnel

Enter the Number of Employees.

What number are full-time? [Q:4.6-14076]

What number are part-time? [Q:4.6-14077]

What number typically are contractors? [Q:4.6-14078]

What number are other types? [Q:4.6-14079]

Enter the Number of Security Officers.

What number are full-time? [Q:4.6-14080]

What number are part-time? [Q:4.6-14081]

What number typically are contractors? [Q:4.6-14082]

What number are other types? [Q:4.6-14083]

Workforce Operations

Work Shifts

Provide a name or short description for each workshift or period.
Add as many workshifts as necessary to account for different starting/ending times and number of employees present.

For each workshift listed, describe facility operations schedule and number of employees.

Workshift Name

| |

Day of Week	Starting Time [Q:4.81-18513]	AM/PM [Q:4.81-18514]	Ending Time [Q:4.81-18515]	AM/PM [Q:4.81-18515]	Number of Employees [Q:4.81-18516]
Monday					
Tuesday					
Wednesday					
Thursday					
Friday					
Saturday					
Sunday					

Workshift Name

| |

Day of Week	Starting Time [Q:4.81-18513]	AM/PM [Q:4.81-18514]	Ending Time [Q:4.81-18515]	AM/PM [Q:4.81-18515]	Number of Employees [Q:4.81-18516]
Monday					
Tuesday					
Wednesday					
Thursday					
Friday					
Saturday					
Sunday					

COI - Chemical Operations

Chemicals of Interest Shipped

Shipment of COI and Other Chemicals

Does the facility ship COI? [Q:5.0-14120]

- ○ Yes
- ○ No

Does the facility ship other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18466]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:5.0-14120] or [Q:5.0-18466], indicate which chemicals are shipped.

Release COI Shipped, Theft/Diversion COI Shipped, Sabotage/Contamination COI Shipped

List each COI present at the facility, and indicate the if the COI is shipped by truck, rail, barge, or pipeline, and indicate the other method if applicable.

Chemical Name	By Truck [Q:5.1-14203], [Q:5.1-14208], [Q:5.1-14213], [Q:5.1-14218], [Q:5.1-14223], [Q:5.1-14228], [Q:5.1-14233]		By Rail [Q:5.1-14204], [Q:5.1-14209], [Q:5.1-14214], [Q:5.1-14219], [Q:5.1-14224], [Q:5.1-14229], [Q:5.1-14234]		By Barge [Q:5.1-14205], [Q:5.1-14210], [Q:5.1-14215], [Q:5.1-14220], [Q:5.1-14225], [Q:5.1-14230], [Q:5.1-14235]		By Pipeline [Q:5.1-18917], [Q:5.1-18919], [Q:5.1-18920], [Q:5.1-18921], [Q:5.1-18922], [Q:5.1-18923], [Q:5.1-18924]		By Other Method [Q:5.1-14206], [Q:5.1-14211], [Q:5.1-14216], [Q:5.1-14221], [Q:5.1-14226], [Q:5.1-14231], [Q:5.1-14236]	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○

Chemical Name	By Truck [Q:5.1-14203], [Q:5.1-14208], [Q:5.1-14213], [Q:5.1-14218], [Q:5.1-14223], [Q:5.1-14228], [Q:5.1-14233]		By Rail [Q:5.1-14204], [Q:5.1-14209], [Q:5.1-14214], [Q:5.1-14219], [Q:5.1-14224], [Q:5.1-14229], [Q:5.1-14234]		By Barge [Q:5.1-14205], [Q:5.1-14210], [Q:5.1-14215], [Q:5.1-14220], [Q:5.1-14225], [Q:5.1-14230], [Q:5.1-14235]		By Pipeline [Q:5.1-18917], [Q:5.1-18919], [Q:5.1-18920], [Q:5.1-18921], [Q:5.1-18922], [Q:5.1-18923], [Q:5.1-18924]		By Other Method [Q:5.1-14206], [Q:5.1-14211], [Q:5.1-14216], [Q:5.1-14221], [Q:5.1-14226], [Q:5.1-14231], [Q:5.1-14236]	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○

Chemicals of Interest Sold

Sale of COI and Other Chemicals

Does the facility sell COI? [Q:5.0-14121]

- ○ Yes
- ○ No

Does the facility sell other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18467]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:5.0-14121] or [Q:5.0-18467, indicate which chemicals are sold.

Chemical Name	Chemical Sold [Q:5.2-14245], [Q:5.2-14247], [Q:5.2-14249], [Q:5.2-14251], [Q:5.2-14253], [Q:5.2-14255], [Q:5.2-14257]	
	Yes	**No**
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○

Select All Industries that the Facility Supplies

Select all industrial clients that apply. [Q:5.2-14258]	**Yes**	**No**
Agricultural	○	○
Electrical	○	○
Energy and Utilities	○	○
Pharmaceutical	○	○
Paints and Coatings	○	○
Mining	○	○
Explosives	○	○
Universities	○	○
Research Institutions	○	○
Plastics	○	○
Healthcare	○	○
Food	○	○
Chemical Manufacturing, Storage, and Distribution	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:5.2-14259]

Chemicals of Interest Receipts

Receipt of COI and Other Chemicals

Does the facility receive COI? [Q:5.0-14119]

- ○ Yes
- ○ No

Does the facility receive other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18468]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:5.0-14119] or [Q:5.0-18468], indicate which chemicals are received.

List each COI present at the facility, and indicate the if the COI is received by truck, rail, barge, or pipeline, and indicate the other method if applicable.

Chemical Name	By Truck [Q:5.3-14152], [Q:5.3-14171], [Q:5.3-14175], [Q:5.3-14179], [Q:5.3-14183], [Q:5.3-14187], [Q:5.3-14191]		By Rail [Q:5.3-14153], [Q:5.3-14172], [Q:5.3-14176], [Q:5.3-14180], [Q:5.3-14184], [Q:5.3-14188], [Q:5.3-14192]		By Barge [Q:5.3-14155], [Q:5.3-14173], [Q:5.3-14177], [Q:5.3-14181], [Q:5.3-14185], [Q:5.3-14189], [Q:5.3-14193]		By Pipeline [Q:5.3-22496], [Q:5.3-22497], [Q:5.3-22499], [Q:5.3-22500], [Q:5.3-22501], [Q:5.3-22502], [Q:5.3-22503]		By Other Method [Q:5.3-14156], [Q:5.3-14174], [Q:5.3-14178], [Q:5.3-14182], [Q:5.3-14186], [Q:5.3-14190], [Q:5.3-14194]	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○

Chemical Name	By Truck [Q:5.3-14152], [Q:5.3-14171], [Q:5.3-14175], [Q:5.3-14179], [Q:5.3-14183], [Q:5.3-14187], [Q:5.3-14191]		By Rail [Q:5.3-14153], [Q:5.3-14172], [Q:5.3-14176], [Q:5.3-14180], [Q:5.3-14184], [Q:5.3-14188], [Q:5.3-14192]		By Barge [Q:5.3-14155], [Q:5.3-14173], [Q:5.3-14177], [Q:5.3-14181], [Q:5.3-14185], [Q:5.3-14189], [Q:5.3-14193]		By Pipeline [Q:5.3-22496], [Q:5.3-22497], [Q:5.3-22499], [Q:5.3-22500], [Q:5.3-22501], [Q:5.3-22502], [Q:5.3-22503]		By Other Method [Q:5.3-14156], [Q:5.3-14174], [Q:5.3-14178], [Q:5.3-14182], [Q:5.3-14186], [Q:5.3-14190], [Q:5.3-14194]	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○
	○	○	○	○	○	○	○	○	○	○

Chemicals of Interest Manufactured

Manufacturing of COI and Other Chemicals

Does the facility manufacture COI? [Q:5.0-14586]

- ○ Yes
- ○ No

Does the facility ship other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18587]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:5.0-14586] or [Q:5.0-18567],, indicate which chemicals are manufactured.

Chemical Name	Chemical Manufactured [Q:5.4-18598], [Q:5.4-18603], [Q:5.4-18608], [Q:5.4-18613], [Q:5.4-18618], [Q:5.4-18623], [Q:5.4-18628]	
	Yes	**No**
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○
	○	○

ASP Upload

CFATS provides all high-risk facilities with the option of submitting an ASP in place of the SSP. DHS may approve an ASP in whole or in part, or subject to revision or supplements, if the ASP meets the requirements of 6 CFR § 27.225.

Do you want to upload an ASP in lieu of using the CSAT SSP? [Q:5.6-17939]

- ○ Yes
- ○ No

If "No" is selected, go to Facility Schematics Upload (page 52).

ASP Upload Measures

Does the ASP address each security/vulnerability issue identified by the facility's SVA, and identify and describe the security measures to address each such security/vulnerability issue? [Q:5.61-18413]

- ○ Yes
- ○ No

Does the ASP identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential mode of terrorist attack? [Q:5.61-18414]

- ○ Yes
- ○ No

Does the ASP identify and describe how security measures selected and utilized by the facility will address each applicable performance standard for the appropriate risk-based tier for the facility? [Q:5.61-18415]

- ○ Yes
- ○ No

Does the ASP provide other information that the Assistant Secretary has deemed necessary, through the DHS Final Notification Letter or other means, regarding facility security? [Q:5.61-18416]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:5.61-18413], [Q:5.61-18414], [Q:5.61-18415], AND [Q:5.61-18416] go to Upload ASP Documents.

ASP Upload Confirmation

The ASP does not address all pertinent factors in 6 CFR 27. Do you wish to upload an ASP in lieu of the CSAT SSP? [Q:5.6.2-18453]

- ○ Yes
- ○ No

If "No" is selected, go to Facility Schematics Upload (page 52).

Upload ASP Documents

Use this page to upload one or more document files.

Enter the name of the ASP document file to upload, then click *Add*. Use names that are distinct enough to easily identify the files. A new entry line will appear for additional ASP files, and a *Describe* button will appear for provision of additional information. Click *Describe* to complete the upload process for each file.

If facility did submit a non-CSAT SVA, what is the date of that submittal? [Q:5.7-18182]

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

Enter names for the ASP files to upload. [Q:5.7-17818]

Filename

Enter a brief description of the uploaded ASP file. [Q:5.72-17826]

Filename

Enter a brief description of the uploaded ASP file. [Q:5.72-17826]

Filename

Enter a brief description of the uploaded ASP file. [Q:5.72-17826]

Facility Schematics Upload

Supporting Documentation

Upload supporting documentation that will assist the evaluation of the SSP.

- Current facility aerial photos and plot plans
- Current facility drawings and system schematics

Do you want to upload facility schematics or photographs that support the SSP?
[Q:5.8-22809]

○ Yes

○ No

If "No" is selected, go to Risk-based Performance Standards (page 55).

Upload Facility Schematics and Photographs

Enter facility schematic or photograph files as needed.
Use this page to upload one or more facility schematic or photograph files.

Facility Schematic Filename

Schematic Filename Description

Select the type of data contained in the file. (Choose one: Aerial photograph, Drawing, Plot plan, System schematic) [Q:5.82-22840]

Enter a brief description of the uploaded facility schematic or photograph file. [Q:5.82-22829].

Facility Schematic Filename

Schematic Filename Description

Select the type of data contained in the file. (Choose one: Aerial photograph, Drawing, Plot plan, System schematic) [Q:5.82-22840]

Enter a brief description of the uploaded facility schematic or photograph file. [Q:5.82-22829].

Facility Schematic Filename

Schematic Filename Description

Select the type of data contained in the file. (Choose one: Aerial photograph, Drawing, Plot plan, System schematic) [Q:5.82-22840]

Enter a brief description of the uploaded facility schematic or photograph file. [Q:5.82-22829].

This page intentionally left blank.

Risk-based Performance Standards

Answer each RBPS (1-18, except for 6 and 7) at the facility level. (Pages 61-304)

If the facility has any Theft/Diversion COI that are listed, answer RBPS 6 at the facility level.

If the facility has any Sabotage COI that are listed, answer RBPS 7 at the facility level. When completed, go to Asset Security Measures.

Asset Security Measures

All assets must be named and described.

Continue adding entries until all applicable assets have been provided. Then provide the requested information.

When describing the asset, provide a brief description of the asset, including the primary function. If the asset is associated with a chemical that is not a COI (e.g., a hazardous material or a potentially dangerous chemical that may be subject to RBPS 5 or 6, respectively), or a chemical identified in the DHS final notification letter, the name of that chemical and the security/vulnerability issue (e.g., release, theft, sabotage) associated with the asset should be described as well.

Asset Name [Q:26.1-14664]

For each listed Asset, copy and answer the questions on the following pages regarding asset level information. (Pages 56-58) When finished, or if none present, go to Completion (Page 59)

Asset Security Measures - Description

List what Asset you are describing.

Provide a brief description of the asset, including the primary function. If the asset is associated with a chemical that is not a COI (e.g., a hazardous material or a potentially dangerous chemical that may be subject to RBPS 5 or 6, respectively), or a chemical identified in the DHS final notification letter, the name of that chemical and the security/vulnerability issue (e.g., release, theft, sabotage) associated with the asset should be described as well. [Q:26.2.-14666]

Is this a critical asset? [Q:26.2.-22738]

- ○ Yes
- ○ No

Is a COI or other chemical from the DHS final notification letter associated with this asset? [Q:26.2-17940]

- ○ Yes
- ○ No

If "No" is selected, go to Select Risk-Based Performance Standards For This Asset

Select All Security/Vulnerability Issues Associated with this Asset
Is the asset associated with release toxic COI listed in the DHS final notification letter? [Q:26.2-14668]

- ○ Yes
- ○ No

Is the asset associated with release flammable COI listed in the DHS final notification letter? [Q:26.2-14669]

- ○ Yes
- ○ No

Is the asset associated with release explosive COI listed in the DHS final notification letter? [Q:26.2-14670]

- ○ Yes
- ○ No

Is the asset associated with theft/diversion explosive/IEDP COI listed in the DHS final notification letter?
[Q:26.2-14671]

- ○ Yes
- ○ No

Is the asset associated with theft/diversion WME COI listed in the DHS final notification letter?
[Q:26.2-14672]

- ○ Yes
- ○ No

Is the asset associated with theft/diversion CW/CWP COI listed in the DHS final notification letter?
[Q:26.2-14673]

- ○ Yes
- ○ No

Is the asset associated with sabotage/contamination COI listed in the DHS final notification letter?
[Q:26.2-14674]

- ○ Yes
- ○ No

List what chemicals of interest (COI) are associated with this asset and the associated type of chemical list the COI belongs to (Toxic, Flammable, Explosive…)

Chemical Name [Q:26.3-14692], [Q:26.3-14694], [Q:26.3-14696], [Q:26.3-14698], [Q:26.3-14700], [Q:26.3-14702], [Q:26.3-14704]	**COI type**

Select Risk-Based Performance Standards For This Asset

If the facility does not have any Theft and Diversion related COI, answer "No" for RBPS 6 [Q:26.4-14718].
If the facility does not have any Sabotage related COI, answer "No" for RBPS 7 [Q:26.4-14719].

Address RBPS 2 for the asset whether or not facility-wide security measures were entered for RBPS 2.

Does the facility implement security measures specific to the asset related to RBPS 3?
[Q:26.4-14715]

- ○ Yes
- ○ No

Does the facility implement security measures specific to the asset related to RBPS 5?
[Q:26.4-14717]

- ○ Yes
- ○ No

Does the facility implement security measures specific to the asset related to RBPS 6?
[Q:26.4-14718]

- ○ Yes
- ○ No

Does the facility implement security measures specific to the asset related to RBPS 7?
[Q:26.4-14719]

- ○ Yes
- ○ No

For each asset, copy each RBPS that you selected "Yes" for, in addition to RBPS 2, and fill out those sections pertaining to that asset.

Completion

SSP Completion

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).

Finish

DHS Communications

A letter acknowledging receipt of the SSP will be sent to the Submitter.

Preparer Copy

Do you want a copy of the letter acknowledging receipt of the SSP to be sent to the Preparer in addition to the Submitter? [Q:1.92-13719]

- ○ Yes
- ○ No

This page intentionally left blank.

RBPS 1 – Restrict Area Perimeter

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed measures for RBPS 1? [Q:7.0-18596]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 1.

Posting (General Data Collection - RBPS 1)

Does the facility have a defined perimeter marked by company property, no trespassing signage, fencing, or other barriers? [Q:7.005-14425]

- ○ Yes
- ○ Partial
- ○ No

If "No" is selected, go to question [Q:7.02-14435], "Does the facility maintain an internal clear zone extending inward from the perimeter barrier?".

Posting (General Data Collection - RBPS 1)

Indicate "Yes" for the perimeter characteristics that apply: [Q:7.01-14429]

Perimeter Characteristic	Yes	No
The perimeter of the facility is posted with company property and no trespassing signage.	○	○
The facility has a perimeter that is defined with a perimeter fence or barrier.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.01-14450]

Clear Zone (RBPS Metric 1.1)

Does the facility maintain an internal clear zone extending inward from the perimeter barrier? [Q:7.02-14435]

- ○ Yes
- ○ Partial
- ○ No

Does the facility maintain an external clear zone extending outward from the perimeter barrier? [Q:7.02-14436]

- ○ Yes
- ○ Partial
- ○ No

If "No" is selected for question [Q:7.02-14435] AND question [Q:7.02-14436] go to question [Q:7.04-14455], "Does the facility maintain a standoff distance for facility assets?")

Clear Zone (RBPS Metric 1.1)

Are the clear zones monitored to ensure that the clear zones remain clear? [Q:7.03-14443]

- ○ Yes
- ○ No

Are violations of the clear zone policy promptly identified and resolved? [Q:7.03-14445]

- ○ Yes
- ○ No

How many feet does the clear zone extend inward from the perimeter barrier? [Q:7.03-14439]

Only answer this question if the answer to question [Q:7.02-14435], "Does the facility maintain an internal clear zone extending inward from the perimeter barrier? " is "Yes" or "Partial"

How many feet does the clear zone extend outward from the perimeter barrier? [Q:7.03-14442]

Only answer this question if the answer to question [Q:7.02-14436], "Does the facility maintain an external clear zone extending outward from the perimeter barrier?" is "Yes" or "Partial"

Standoff Distance (RBPS Metric 1.3)

Does the facility maintain a standoff distance for facility assets? [Q:7.04-14455]

- ○ Yes
- ○ Partial
- ○ No

Additional comments: [Q:7.04-14456]

Topographical Barriers (RBPS Metric 1.1)

Select "Yes" for all the topographical barriers that the facility has: [Q:7.05-14469]

Topographical Barrier	Yes	Partial	No
Mountains/cliffs	○	○	○
Swamp/wetlands	○	○	○
Forest/woodlands	○	○	○
Valleys	○	○	○
Bodies of water/rivers	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.05-14474]

Landscaping Barriers (RBPS Metric 1.1 and 1.2)

Select "Yes" for all the landscaping barriers that the facility has: [Q:7.05-14471]

Landscaping Barrier	Yes	Partial	No
Hedge row	○	○	○
Planter	○	○	○
Slalom or serpentine chicane	○	○	○
Retaining wall	○	○	○
Revetment	○	○	○
Rocks	○	○	○
Timbers	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.05-14475]

Vegetation (RBPS Metric 1.1)

Which of the following best describes the vegetation control program for clear zones and perimeter barriers? [Q:7.05-14473]

- ○ No specific clear zone
- ○ Casual clear zone
- ○ Strict clear zone
- ○ Other

If "Other" is selected, enter a description: [Q:7.05-14488]

Fence (RBPS Metric 1.1)

Select "Yes" for all the fence barriers that the facility utilizes: [Q:7.06-14479]

Fence Barrier	Yes	Partial	No
Chain Link	○	○	○
Metal	○	○	○
Decorative ironwork	○	○	○
Vinyl	○	○	○
Concrete	○	○	○
Wood	○	○	○
Extruded metal sheeting	○	○	○
Other	○	○	○

If "No" selected for all barriers, go to Wall (RBPS Metric 1.1)

If "Other" is selected, enter a description: [Q:7.06-14484]

Fence Top Guard (RBPS Metric 1.1)

If "No" is selected for all barriers in question [Q:7.06-14479], skip to question [Q:7.08-14489]

Select "Yes" for all the fence top guards that the facility utilizes: [Q:7.07-14483]

Fence Top Guard	Yes	Partial	No
Electrified wire	○	○	○
Break-away/floppy top guard	○	○	○
Razor-wire	○	○	○
Concertina wire	○	○	○
Barbed wire, barbed tape, razor wire	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.07-14486]

Wall (RBPS Metric 1.1)

Select "Yes" for all the wall types that the facility utilizes: [Q:7.08-14489]

Wall Type	Yes	Partial	No
Poured concrete	○	○	○
Concrete masonry unit	○	○	○
Brick	○	○	○
Stucco	○	○	○
Wood	○	○	○
Metal Panel	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.08-14490]

Gate/Door (RBPS Metric 1.1)

Does the facility perimeter barrier have any gates? [Q:7.09-14491]

○ Yes
○ No

Does the facility perimeter barrier have any doors? [Q:7.09-14492]

○ Yes
○ No

If "No" is selected for both question [Q:7.09-14491] AND question [Q:7.09-14492], go to Anti-Personnel (General Data Collection RBPS 1)

Gate (RBPS Metric 1.1)

If "No" is selected for question [Q:7.09-14491] , go to Door (RBPS Metric 1.1)

Select "Yes" if the facility has gates of this material: [Q:7.1-14495]

Gate Material	Yes	Partial	No
Chain link	○	○	○
Metal, solid	○	○	○
Metal, mesh	○	○	○
Wood	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.1-14496]

Select "Yes" if the facility uses this hardware in conjunction with the facility gates: [Q:7.1-14500]

Gate Hardware	Yes	Partial	No
Self-latching deadbolt	○	○	○
Locking latchset	○	○	○
Fork latch, lockable	○	○	○
Drop rod, lockable	○	○	○
Chain and padlock, casehardened	○	○	○
Magnetic lock	○	○	○
Chain and padlock, non-casehardened	○	○	○
Remote mechanical lock	○	○	○
Emergency egress (crash-out) hardware	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.1-14499]

Door (RBPS Metric 1.1)

If "No" is selected for question [Q:7.09-14492] , go to Anti-Personnel (General Data Collection RBPS 1)

Select "Yes" if the facility has doors of this material: [Q:7.1-14497]

Door Material	Yes	Partial	No
Chain link	○	○	○
Metal, solid	○	○	○
Metal, mesh	○	○	○
Wood	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.1-14498]

Select "Yes" if the facility uses this hardware in conjunction with the facility doors: [Q:7.1-14501]

Door Hardware	Yes	Partial	No
No exposed locking hardware	○	○	○
Lockset, cylinder	○	○	○
Lockset, mortise	○	○	○
Deadbolt	○	○	○
Magnetic lock	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.1-14502]

Anti-Personnel (General Data Collection RBPS 1)

Select "Yes" if the facility has the anti-personnel barrier: [Q:7.13-14505]

Anti-Personnel Barrier	Yes	Partial	No
Barbed wire (on the ground)	○	○	○
Concertine wire (on the ground)	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.13-14506]

Access Points (General Data Collection RBPS 1)

Select "Yes" if the access point exists at the facility: [Q:7.14-14507]

Access Point	Yes	No
Drainage structures	○	○
Culverts	○	○
Ditches	○	○
Pipelines	○	○
Public roadways	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.14-14508]

Intrusion Detection (RBPS Metric 1.4)

Does the facility utilize an intrusion detection system which operates using intrusion detection sensors to detect attempts to enter the facility perimeter? [Q:7.15-14509]

- ○ Yes
- ○ Partial
- ○ No

If "No" is selected, go to Personnel-Based (General Data Collection RBPS 1).

Intrusion Detection (RBPS Metric 1.4)

Does the intrusion detection system have a backup power supply? [Q:7.16-14548]

- ○ Yes
- ○ No

Select "Yes" if the area is covered by intrusion detection system sensors: [Q:7.16-14510]

Facility Area	Yes	No
The perimeter barriers and entry points are covered by intrusion detection sensors to detect attempts to enter the facility perimeter.	○	○
Building walls, doors, windows, etc. that make up portions of the perimeter barrier are covered by intrusion detection sensors to detect attempts to enter the facility perimeter.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.16-14511]

IDS Integration (RBPS Metric 1.4)

Select "Yes" if the intrusion detection system is associated with the area: [Q:7.16-14512]

Facility Area	Yes	No
The intrusion detection system is integrated with the access control system.	○	○
The intrusion detection system is integrated with a surveillance system.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.16-14539]

Where can the system be controlled? [Q:7.16-14632]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:7.16-14633]

Where can the system be administrated? [Q:7.16-14634]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:7.16-14635]

Select "Yes" if the intrusion detection system is monitored in the location: [Q:7.16-14654]

Monitoring Location	Yes	No
Local, at the facility	○	○
Another company facility	○	○
Remote, by third-party	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.16-14655]

What is the monitoring frequency of the intrusion detection system? [Q:7.16-14638]

- ○ Monitoring frequency is continuous
- ○ Monitoring frequency is periodic (at least 50% of the time)
- ○ Other

If "Other" is selected, enter a description: [Q:7.16-14639]

Intrusion Detection (RBPS Metric 1.4)

Select "Yes" if the sensor in use at the facility: [Q:7.17-14525]

Fence Mounted Sensor	Yes	Partial	No
Capacitance sensor	○	○	○
E-field sensor	○	○	○
Fiber-optic cables	○	○	○
Strain-sensitive	○	○	○
Taut wire sensor	○	○	○
Vibration-detection sensors	○	○	○
Fence mounted sensors have a backup power supply	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.17-14640]

Select "Yes" if the sensor in use at the facility: [Q:7.17-14527]

Volumetric Sensor	Yes	No
Acoustic sensor	○	○
Active infrared	○	○
Buried balanced pressure	○	○
Buried fiber optic	○	○
Buried geophone	○	○
Buried line sensors	○	○
Dual technology (IR/microwave)	○	○
Intelligent video	○	○
Mono-static or bi-static microwave sensors	○	○
Passive infrared	○	○
Passive ultrasonic	○	○
Ported coaxial cable	○	○
Radar	○	○
Video motion detection	○	○
Volumetric sensors have a backup power supply.	○	○
Other	○	○

If “Other” is selected, enter a description: [Q:7.17-14641]

Select "Yes" if the sensor in use at the facility: [Q:7.17-14529]

Beam Sensor	Yes	No
Photoelectric beam	○	○
Infrared (IR) beam	○	○
Beam sensors have a backup power supply.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.17-14642]

Select "Yes" if the sensor in use at the facility: [Q:7.17-14531]

Wall Mounted Sensor	Yes	Partial	No
Vibration sensor	○	○	○
Fiber optic wall	○	○	○
Wall mounted sensors have backup power supply	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.17-14643]

Select "Yes" if the sensor in use at the facility: [Q:7.17-14533]

Gate/Door Sensor	Yes	Partial	No
Magnetic switch	○	○	○
Balanced magnetic switch	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.17-14644]

Window Mounted Sensor	Select "Yes" if the sensor in use at the facility: [Q:7.17-14535]			Does this sensor have a backup power supply?: [Q:7.17-14536]	
	Yes	Partial	No	Yes	No
Glassbreak, mechanical	○	○	○	○	○
Glassbreak, acoustical	○	○	○	○	○
Window mounted sensors have backup power supply	○	○	○	○	○
Other	○	○	○	○	○

If "Other" is selected, enter a description: [Q:7.17-14537]

Personnel-Based (General Data Collection RBPS 1)

Select "Yes" if the facility has this type of site personnel: [Q:7.18-14542]

Personnel Category	Yes	No
Protective forces, dedicated posts/positions	○	○
Protective force, roving patrol	○	○
Operators, dedicated posts/positions	○	○
Operators, roving rounds	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.18-14543]

CCTV (RBPS Metric 1.4)

Does the facility utilize a CCTV system for facility surveillance? [Q:7.19-14547]

- ○ Yes
- ○ No

If "No" is selected, go to Mobile Patrols (RBPS Metric 1.4).

CCTV (RBPS Metric 1.4)

Does the CCTV system cover the area?: [Q:7.2-14555]

Area	Yes	Partial	No	Not Applicable
The site provides direct and remote surveillance at critical locations identified in the SVA to detect sabotage.	○	○	○	○
Surveillance is provided for loading areas.	○	○	○	○
Surveillance is provided for unloading areas.	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:7.2-14556]

Where can the CCTV system be controlled? [Q:7.2-14569]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:7.2-14570]

Where can the CCTV system be administered? [Q:7.2-14571]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:7.2-14572]

Is the CCTV system monitored here? [Q:7.2-14573]

Location	Yes	No
Local, at the facility	○	○
Another company facility	○	○
Remote, by third-party	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.2-14574]

Which best describes the CCTV system monitoring frequency? [Q:7.2-14577]

- ○ Monitoring frequency is continuous
- ○ Monitoring frequency is periodic (at least 50% of the time)
- ○ Other

If "Other" is selected, enter a description: [Q:7.2-14578]

CCTV (RBPS Metric 1.4)

Does the facility use the CCTV feature? [Q:7.21-14583]

Camera Technology	Yes	Partial	No
No light level	○	○	○
Low light level	○	○	○
Day/night switching	○	○	○
Color	○	○	○
Black and white	○	○	○
Infrared imaging	○	○	○
Thermal imaging	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.21-14584]

Does the facility use the CCTV feature? [Q:7.21-14585]

Camera Type	Yes	Partial	No
Fixed view	○	○	○
Pan-tilt-zoom view	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.21-14586]

Does the facility use the CCTV feature? [Q:7.21-14587]

Camera Communication	Yes	Partial	No
Analog/coaxial	○	○	○
Digital, wired	○	○	○
Digital, wired with Power Over Ethernet (PoE)	○	○	○
Digital, wireless	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.21-14588]

Does the facility use the CCTV feature? [Q:7.21-14589]

Camera Controller	Yes	Partial	No
Digital recording/controller combination	○	○	○
Direct camera control	○	○	○
Matrix switcher	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:7.21-14590]

Mobile Patrols (RBPS Metric 1.4)

Indicate "Yes" for the type of mobile patrols utilized at the facility: [Q:7.27-14609]

Mobile Post	Yes	No	Not Applicable
Foot patrols	○	○	○
Vehicle patrols	○	○	○
K-9 patrols	○	○	○
Waterborne patrols	○	○	○
Airborne patrols	○	○	○
Other mobile posts	○	○	○

If "Other" is selected, enter a description: [Q:7.27-23034]

Posted Personnel (RBPS Metric 1.4)

Are security personnel used to provide surveillance of areas and identify unauthorized activities and/or access to materials? [Q:7.28-14613]

○ Yes

○ No

Do the posted personnel provide the observation? [Q:7.28-14611]

Observation	Yes	No
Person(s) provide dedicated observation at a single location.	○	○
Person(s) provide casual observation at a single location.	○	○
Person(s) provide dedicated observation while roving.	○	○
Person(s) provide casual observation while roving.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:7.28-14616]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:7.3-14651]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:7.31-14652]

For more information, refer to the SSP instructions.

RBPS 2 – Secure Site Assets

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed measures for RBPS 2? [Q:8.0-18661, Q:28.0-18756]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 2
If answering at the Asset level, write the name of the asset for which you are providing answers.

If answering at the Asset level, go to Restricted/Secure Areas (General Data Collection RBPS 2)

Facility Security Measures

Does the facility have facility-wide security measures for RBPS 2? [Q:8.005-18873]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 2.

Asset Security Measures

Does the facility have asset-specific security measures for RBPS 2 that are different from the facility-wide security measures for RBPS 2? [Q:8.005-17932]

- ○ Yes
- ○ No

Restricted/Secure Areas (General Data Collection RBPS 2)

Does the facility define restricted/secure areas for assets within the perimeter of the facility? [Q:8.01-14860, Q:28.01-16029]

- ○ Yes
- ○ No

If "No" is selected, go to Standoff Distance (RBPS Metric 2.3).

Restricted Area - General (RBPS Metric 2.1)

Select "Yes" if the statement applies to the facility regarding restricted areas: [Q:8.02-14972, Q:28.02-16030]

Classification	Yes	Partial	No
Restricted areas are defined by barriers at least equivalent to the perimeter barrier for the facility.	○	○	○
Access into restricted areas is limited to authorized individuals.	○	○	○
Doors/gates into restricted areas are secured when the area is not occupied by an authorized individual.	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.02-14973, Q:28.02-16031]

Standoff Distance (RBPS Metric 2.3)

Does the facility maintain a standoff distance for facility assets? [Q:8.03-14974, Q:28.03-16032]

○ Yes
○ No
○ Other

If "Other" is selected, enter a description: [Q:8.03-14975, Q:28.03-16033]

Fence (RBPS Metric 2.1)

Select "Yes" for all the fence barriers that the facility utilizes: [Q:8.04-14976, Q:28.04-16034]

Fence Barrier	Yes	Partial	No
Chain Link	○	○	○
Metal	○	○	○

Fence Barrier	Yes	Partial	No
Decorative ironwork	○	○	○
Vinyl	○	○	○
Concrete	○	○	○
Wood	○	○	○
Extruded metal sheeting	○	○	○
Other	○	○	○

If "No" is selected for all barriers, go to Wall (RBPS Metric 2.1).

If "Other" is selected, enter a description: [Q:8.04-14977, Q:28.04-16035]

Fence Top Guard (RBPS Metric 2.1)

If "No" is selected for all barriers in question [Q:8.04-14976] , go to Wall (RBPS Metric 2.1).

Select "Yes" for all the fence top guards that the facility utilizes: [Q:8.05-14985, Q:28.05-16037]

Fence Top Guard	Yes	Partial	No
Electrified wire	○	○	○
Break-away/floppy top guard	○	○	○
Razor-wire	○	○	○
Concertina wire	○	○	○
Barbed wire, barbed tape, razor wire	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.05-14986, Q:28.05-16038]

Wall (RBPS Metric 2.1)

Select "Yes" for all the wall types that the facility utilizes: [Q:8.06-14999, Q:28.06-16039]

Wall Type	Yes	Partial	No
Poured concrete	○	○	○
Concrete masonry unit	○	○	○
Brick	○	○	○
Stucco	○	○	○
Wood	○	○	○
Metal Panel	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.06-15000, Q:28.06-16040]

Gate/Door (RBPS Metric 2.1)

Does the facility secure site assets have any gates?, Does the asset have any gates?
[Q:8.07-14997, Q:28.07-16041]

○ Yes
○ No

Does the facility secure site assets have any doors?, Does the asset have any doors?
[Q:8.07-14998, Q:28.07-16042]

○ Yes
○ No

If "No" is selected for both question [Q:8.07-14997] AND question [Q:8.07-14998], go to Locking/Control Devices (RBPS Metric 2.1).

Gate (RBPS Metric 2.1)

If "No" is selected for question [Q:8.07-14997] *go to Door (RBPS Metric 2.1).*

Select "Yes" if the secure site assets have gates of this material: [Q:8.08-15003, Q:28.08-16045]

Gate Material	Yes	Partial	No
Chain link	○	○	○
Metal, solid	○	○	○
Metal, mesh	○	○	○
Wood	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.08-15004, Q:28.08-16046]

Select "Yes" if the secure site assets use this hardware in conjunction with the secure site asset gates: [Q:8.08-15005, Q:28.08-16047]

Gate Hardware	Yes	Partial	No
Self-latching deadbolt	○	○	○
Locking latchset	○	○	○
Fork latch, lockable	○	○	○
Drop rod, lockable	○	○	○
Chain and padlock, casehardened	○	○	○
Magnetic lock	○	○	○
Chain and padlock, non-casehardened	○	○	○
Remote mechanical lock	○	○	○
Emergency egress (crash-out) hardware	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.08-15006, Q:28.08-16048]

Door (RBPS Metric 2.1)

If "No" is selected for question [Q:8.07-14998], go to Locking/Control Devices (RBPS Metric 2.1).

Select "Yes" if the secure site assets have doors of this material: [Q:8.08-15007, Q:28.08-16049]

Door Material	Yes	Partial	No
Wood, hollow core	○	○	○
Solid core door	○	○	○
Fire-rated door	○	○	○
Industrial metal door	○	○	○
Blast resistant exterior doors	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.08-15008, Q:28.08-16050]

Select "Yes" if the secure site assets use this hardware in conjunction with the secure site asset doors: [Q:8.08-15009, Q:28.08-16051]

Door Hardware	Yes	Partial	No
No exposed locking hardware	○	○	○
Lockset, cylinder	○	○	○
Lockset, mortise	○	○	○
Deadbolt	○	○	○
Magnetic lock	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.08-15010, Q:28.08-16052]

Locking/Control Devices (RBPS Metric 2.1)

Select "Yes" if the secure site assets have the locking/control device: [Q:8.09-15047, Q:28.09-16054]

Locking/Control Device	Yes	Partial	No
Magnetic locks	○	○	○
Gate operators	○	○	○
Electric strike	○	○	○
Movable barrier controllers	○	○	○
Electric lockset	○	○	○
Electrified panic hardware	○	○	○
Electric deadbolt	○	○	○
Locking/control devices have a backup power supply	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.09-15046, Q:28.09-16055]

Ceiling/Roof (RBPS Metric 2.1)

Does the facility have grilles or other barriers at skylights and louvers over 96 square inches? [Q:8.1-15048, Q:28.1-16056]

○ Yes
○ No
○ Other

If "Other" is selected, enter a description: [Q:8.1-15049, Q:28.1-16057]

Internal Barriers (RBPS Metric 2.1)

Select "Yes" for all the barrier classifications that the secure site assets utilize: [Q:8.11-15050, Q:28.11-16058]

Barrier Classification	Yes	Partial	No
Fixed or active barriers, (e.g., doors, vaults, three-point locks)	○	○	○
Manually-activated barriers, (e.g., dispensed liquids, foams)	○	○	○
Sensor-activated barriers, (e.g., dispensed liquids, foams)	○	○	○
Facility has backup power supply for internal barriers	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.11-15051, Q:28.11-16059]

Barrier Upgrades (RBPS Metric 2.1)

Select "Yes" for all the barrier upgrades that the secure site assets utilize: [Q:8.12-15052, Q:28.12-16060]

Barrier Upgrade	Yes	Partial	No
Grates placed on culverts inside the facility	○	○	○
Manholes are locked with security fastener/lock	○	○	○
Hardened site openings larger than 96 square inches	○	○	○
Enhanced climb/cut resistant fencing or walls	○	○	○

Barrier Upgrade	Yes	Partial	No
Foundation enhancements for fencing to prevent tunneling	○	○	○
Burglar-resistant glass	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.12-15053, Q:28.12-16061]

Anti-Vehicle (RBPS Metric 2.2)

Anti-Vehicle Measure	What is the DOS K Rating on the anti-vehicle measure? [Q:8.135-15054, Q:28.135-18848] (Choose One: Not Applicable, DOS K Rating 0, DOS K Rating 4, DOS K Rating 8, DOS K Rating 12, Other, Unknown)	Does the measure have a backup power supply? [Q:8.135-18845, Q:28.135-18850]		
		Yes	No	Not Applicable
Berm		○	○	○
Anti-vehicle cable		○	○	○
Beam		○	○	○
Bollard		○	○	○
Cable-beam / Cantilever		○	○	○
Drop arm		○	○	○
K-rail		○	○	○
Embankment		○	○	○
Jersey barrier		○	○	○
Wedge		○	○	○
Vehicle capture net		○	○	○
Case-hardened chains and locks		○	○	○
Planter		○	○	○
Chain link gate reinforcement		○	○	○

Anti-Vehicle Measure	What is the DOS K Rating on the anti-vehicle measure? [Q:8.135-15054, Q:28.135-18848] (Choose One: Not Applicable, DOS K Rating 0, DOS K Rating 4, DOS K Rating 8, DOS K Rating 12, Other, Unknown)	Does the measure have a backup power supply? [Q:8.135-18845, Q:28.135-18850]		
		Yes	No	Not Applicable
Cable barriers		○	○	○
Drum and cable barriers		○	○	○
Dragnet		○	○	○
Removable nuisance barrier		○	○	○
Guardrail		○	○	○
Motorized barricade		○	○	○
Hydraulic barricade		○	○	○
Electronic barrier gate		○	○	○
Tire-penetrating traffic barrier (One way tire trendles)		○	○	○
Portable roadblock tire-puncturing device		○	○	○
Other		○	○	○

If "Other" is selected, enter a description of the "Other" measure: [Q:8.135-15055, Q:28.135-18851]

Intrusion Detection (RBPS Metric 2.4)

Does the facility utilize an intrusion detection system which operates using intrusion detection sensors to detect attempts to enter the facility perimeter? [Q:8.15-15061, Q:28.15-16067]

- ○ Yes
- ○ Partial
- ○ No

If "No" is selected, go to Personnel-Based (RBPS Metric 2.4).

Intrusion Detection (RBPS Metric 2.4)

Does the intrusion detection system have a backup power supply? [Q:8.16-15062, Q:28.16-16073]

- ○ Yes
- ○ No

Select "Yes" if the area is covered by intrusion detection system sensors: [Q:8.16-15063, Q:28.16-16074]

Facility Area	Yes	Partial	No
The perimeter barriers and entry points are covered by intrusion detection sensors to detect attempts to enter the facility perimeter.	○	○	○
Building walls, doors, windows, etc. that make up portions of the perimeter barrier are covered by intrusion detection sensors to detect attempts to enter the facility perimeter.	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:8.16-15064, Q:28.16-16075]

IDS Integration (RBPS Metric 2.4)

Select "Yes" if the intrusion detection system is associated with the area: [Q:8.16-15065, Q:28.16-16076]

Facility Area	Yes	No
The intrusion detection system is integrated with the access control system.	○	○
The intrusion detection system is integrated with a surveillance system.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.16-15066, Q:28.16-16077]

Where can the system be controlled? [Q:8.16-15067, Q:28.16-16078]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:8.16-15068, Q:28.16-16079]

Where can the system be administrated? [Q:8.16-15069, Q:28.16-16080]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:8.16-15070, Q:28.16-16081]

Select "Yes" if the intrusion detection system is monitored in the location: [Q:8.16-15071, Q:28.16-16068]

Monitoring Location	Yes	No
Local, at the facility	○	○
Another company facility	○	○
Remote, by third-party	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.16-15072]

What is the monitoring frequency of the intrusion detection system? [Q:8.16-15073, Q:28.16-16070]

- ○ Monitoring frequency is continuous
- ○ Monitoring frequency is periodic (at least 50% of the time)
- ○ Other

If "Other" is selected, enter a description: [Q:8.16-15074, Q:28.16-16071]

Intrusion Detection (RBPS Metric 2.4)

Select "Yes" if the sensor in use at the facility: [Q:8.17-15075, Q:28.17-16082]

Fence Mounted Sensor	Yes	No
Capacitance sensor	○	○
E-field sensor	○	○
Fiber-optic cables	○	○
Strain-sensitive	○	○
Taut wire sensor	○	○
Vibration-detection sensors	○	○
Fence mounted sensors have a backup power supply	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.17-15077, Q:28.17-16084]

Select "Yes" if the sensor in use at the facility: [Q:8.17-15078, Q:28.17-16085]

Volumetric Sensor	Yes	No
Acoustic sensor	○	○
Active infrared	○	○
Buried balanced pressure	○	○
Buried fiber optic	○	○
Buried geophone	○	○
Buried line sensors	○	○
Dual technology (IR/microwave)	○	○
Intelligent video	○	○
Mono-static or bi-static microwave sensors	○	○
Passive infrared	○	○
Passive ultrasonic	○	○

Volumetric Sensor	Yes	No
Ported coaxial cable	○	○
Radar	○	○
Video motion detection	○	○
Volumetric sensors have a backup power supply.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.17-15080, Q:28.17-16087]

Select "Yes" if the sensor in use at the facility: [Q:8.17-15081, Q:28.17-16088]

Beam Sensor	Yes	No
Photoelectric beam	○	○
Infrared (IR) beam	○	○
Beam sensors have a backup power supply.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.17-15083, Q:28.17-16090]

Select "Yes" if the sensor in use at the facility: [Q:8.17-15084, Q:28.17-16091]

Wall Mounted Sensor	Yes	No
Vibration sensor	○	○
Fiber optic wall	○	○
Wall mounted sensors have backup power supply	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.17-15086, Q:28.17-16093]

Select "Yes" if the sensor in use at the facility: [Q:8.17-15087, Q:28.17-16094]

Gate/Door Sensor	Yes	No
Magnetic switch	○	○
Balanced magnetic switch	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.17-15089, Q:28.17-16096]

Window Mounted Sensor	Select "Yes" if the sensor in use at the facility: [Q:8.17-15090, Q:28.17-16097]		Does this sensor have a backup power supply? [Q:8.17-15091, Q:28.17-16098]	
	Yes	No	Yes	No
Glassbreak, mechanical	○	○	○	○
Glassbreak, acoustical	○	○	○	○
Window mounted sensors have backup power supply	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:8.17-15092, Q:28.17-16099]

Personnel-Based (RBPS Metric 2.4)

Select "Yes" if the facility has this type of site personnel: [Q:8.18-15094, Q:28.18-16101]

Personnel Category	Yes	No
Protective forces, dedicated posts/positions	○	○
Protective force, roving patrol	○	○
Operators, dedicated posts/positions	○	○
Operators, roving rounds	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.18-15095, Q:28.18-16102]

CCTV (RBPS Metric 2.4)

Does the facility utilize a CCTV system for facility surveillance? [Q:8.19-15096, Q:28.19-16103]

○ Yes
○ No

If "No" is selected, go to Security Lighting (RBPS Metric 2.4).

CCTV (RBPS Metric 2.4)

Does the CCTV system have a backup power supply? [Q:8.2-15097, Q:28.2-16104]

○ Yes
○ No

Does the CCTV system cover the area?: [Q:8.2-15098, Q:28.2-16105]

Area	Yes	Partial	No	Not Applicable
The site provides direct and remote surveillance at critical locations identified in the SVA to detect sabotage.	○	○	○	○
Surveillance is provided for loading areas.	○	○	○	○

Area	Yes	Partial	No	Not Applicable
Surveillance is provided for unloading areas.	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:8.2-15099, Q:28.2-16106]

Is the surveillance system integrated with the access control system? [Q:8.2-15100, Q:28.2-16107]

○ Yes
○ No

Is the surveillance system integrated with the intrusion detection system? [Q:8.2-15101, Q:28.2-16108]

○ Yes
○ No

Are there any other systems that the CCTV system is associated with? [Q:8.2-15102, Q:28.2-16109]

○ Yes
○ No

If "Other" is selected, enter a description: [Q:8.2-15103, Q:28.2-16110]

Where can the CCTV system be controlled? [Q:8.2-15104, Q:28.2-16111]

○ Local at the facility
○ Another company facility
○ Remote by third-party contractor
○ Other
○ Not Applicable

If "Other" is selected, enter a description: [Q:8.2-15105, Q:28.2-16112]

Where can the CCTV system be administered? [Q:8.2-15106, Q:28.2-16113]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:8.2-15107, Q:28.2-16114]

Is the CCTV system monitored here? [Q:8.2-15108, Q:28.2-16115]

Location	Yes	No
Local, at the facility	○	○
Another company facility	○	○
Remote, by third-party	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.2-15109, Q:28.2-16116]

What best describes how the CCTV system is staffed and monitored? [Q:8.2-15110, Q:28.2-16117]

- ○ System monitoring and control by dedicated control room operator.
- ○ System monitoring an ancillary responsibility of control room operator.
- ○ System monitoring and control by dedicated security force member.
- ○ System monitoring an ancillary responsibility of security force member.
- ○ Other

If "Other" is selected, enter a description: [Q:8.2-15111, Q:28.2-16118]

Which best describes the CCTV system monitoring frequency? [Q:8.2-15112, Q:28.2-16119]

- ○ Monitoring frequency is continuous
- ○ Monitoring frequency is periodic (at least 50% of the time)
- ○ Other

CCTV Facility Coverage (RBPS Metric 2.4)

Enter the percent of the perimeter fencing monitored via CCTV. [Q:8.2-15114, Q:28.2-16121

Enter the percent of gates that are monitored via CCTV. [Q:8.2-15115, Q:28.2-16122]

Enter the percent of critical locations (loading/unloading areas, storage vessels, etc.) monitored via CCTV. [Q:8.2-15116, Q:28.2-16123]

CCTV (RBPS Metric 2.4)

Does the facility use the CCTV feature? [Q:8.21-15125, Q:28.21-16125]

Camera Technology	Yes	No
No light level	○	○
Low light level	○	○
Day/night switching	○	○
Color	○	○
Black and white	○	○
Infrared imaging	○	○
Thermal imaging	○	○

Camera Technology	Yes	No
Other	○	○

If "Other" is selected, enter a description: [Q:8.21-15126, Q:28.21-16126]

Does the facility use the CCTV feature? [Q:8.21-15127, Q:28.21-16127]

Camera Type	Yes	No
Fixed view	○	○
Pan-tilt-zoom view	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.21-15128, Q:28.21-16128]

Does the facility use the CCTV feature? [Q:8.21-15129, Q:28.21-16129]

Camera Communication	Yes	No
Analog/coaxial	○	○
Digital, wired	○	○
Digital, wired with Power Over Ethernet (PoE)	○	○
Digital, wireless	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.21-15130, Q:28.21-16130]

Does the facility use the CCTV feature? [Q:8.21-15131, Q:28.21-16131]

Camera Controller	Yes	No
Digital recording/controller combination	○	○
Direct camera control	○	○
Matrix switcher	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.21-15132, Q:28.21-16132]

Does the facility use the CCTV feature? [Q:8.21-15133, Q:28.21-16133]

Recording Medium	Yes	No
Analog/tape	○	○
Digital	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:8.21-15134, Q:28.21-16134]

Security Lighting (RBPS Metric 2.4)

Does the facility provide and maintain sufficient illumination levels to permit security and facility personnel to safely perform their duties and permit the surveillance of the facility?
[Q:8.22-15135, Q:28.22-16135]

○ Yes
○ No

If "No" is selected, go to Mobile Patrols (RBPS Metric 2.4).

Security Lighting (RBPS Metric 2.4)

Does the security lighting have a backup power supply? [Q:8.23-15160, Q:28.23-16136]

- ○ Yes
- ○ No

Lighting Area	Indicate the brightness of the security area. [Q:8.24-15164, Q:28.24-16141]	Indicate lighting units. [Q:8.24-18886, Q:28.24-18890] (Choose Lumens or Foot-candles)
The facility provides and maintains sufficient illumination levels to permit security and facility personnel to safely perform their duties and permit the surveillance of the facility.		
General street lighting		
Site perimeter lighting		
Security-specific lighting		
Operational lighting		
Portable lighting		
Security gates lighting		
Critical locations lighting		
Other		

If "Other" is selected, enter a description: [Q:8.23-15162, Q:28.23-16138]

What percentage of the security gates are covered? [Q:8.24-15165, Q:28.24-16175]

Only answer this question if "Security Gates Lighting" is one of the selections for question [Q:8.24-15164], "Indicate the brightness of the security area"

What percentage of the critical locations are covered? [Q:8.24-15166, Q:28.24-16177]

Only answer this question if "Critical Locations Lighting" is one of the selections for question [Q:8.24-15164], "Indicate the brightness of the security area"

Mobile Patrols (RBPS Metric 2.4)

Indicate "Yes" for the type of mobile patrols utilized at the facility: [Q:8.27-15173, Q:28.27-16150]

Mobile Post	Yes	No	Not Applicable
Foot patrols	○	○	○
Vehicle patrols	○	○	○
K-9 patrols	○	○	○
Waterborne patrols	○	○	○
Airborne patrols	○	○	○
Other mobile posts	○	○	○

If "Other" is selected, enter a description: [Q:8.27-23037, Q:28.27-16151]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:8.88-14883, Q:28.88-16154]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:8.89-14884, Q:28.89-16155]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 3 – Screening and Access Control

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 3?
[Q:9.0-18663, Q:29.0-18764]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 3
If answering at the Asset level, write the name of the asset for which you are providing answers.

If answering at the Asset level, go to Screening for Facility Access (RBPS Metric 3.4)

Facility Security Measures

Does the facility have facility-wide security measures for RBPS 3?
[Q:9.004-18841]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 3.

Asset Security Measures

Does the facility have asset-specific security measures for RBPS 3 that are different from the facility-wide security measures for RBPS 3?
[Q:9.004-17933]

- ○ Yes
- ○ No

Screening for Facility Access (RBPS Metric 3.4)

What type of overall screening is performed at the facility?
[Q:9.005-15590, Q:29.005-17089]

- ○ Facility screens all personnel and vehicles entering facility.
- ○ Facility screens 75% of personnel and 75% of vehicles entering facility.
- ○ Facility screens 50% of personnel and 50% of vehicles entering facility.
- ○ Facility screens 25% of personnel and 25% of vehicles entering facility.
- ○ Facility screens <25% of personnel and <25% of vehicles entering facility.
- ○ Facility does not screen personnel or vehicles entering facility.
- ○ Other

If "Other" is selected, enter a description. [Q:9.005-15591, Q:29.005-17090]

Screening for Restricted Area Access (RBPS Metric 3.4)

What type of screening is performed at facility-designated restricted areas?
[Q:9.005-15608, Q:29.005-17091]

- ○ Facility screens all personnel and all vehicles entering facility-designated restricted areas.
- ○ Facility screens high percentage of personnel and vehicles entering facility-designated restricted areas.
- ○ Facility screens selected personnel and vehicles entering facility-designated restricted areas.
- ○ Facility does not screen personnel and vehicles entering facility designated restricted areas.
- ○ Other

If "Other" is selected, enter a description. [Q:9.005-15609, Q:29.005-17092]

If "Facility does not screen personnel and vehicles entering facility-designated restricted area" is selected for question [Q:9.005-15608, Q:29.005-17091, go to Identification Verification System (RBPS Metric 3.1)

Inspection Capabilities (RBPS Metric 3.4)

Does the facility inspect vehicles seeking access to the facility?
[Q:9.01-15875, Q:29.01-17110]

- ○ Yes
- ○ No

Does the facility inspect items hand carried by individuals seeking access to the facility?
[Q:9.01-15881, Q:29.01-17111]

- ○ Yes
- ○ No

Does the facility inspect outbound vehicles leaving restricted areas that contain Theft COI?
[Q:9.01-15882, Q:29.01-17112]

- ○ Yes
- ○ No

Does the facility inspect outbound items hand carried by individuals leaving restricted areas that contain Theft COI?
[Q:9.01-15884, Q:29.01-17113]

- ○ Yes
- ○ No

If "Yes" is answered to [Q:9.01-15875, Q:29.01-17110] or [Q:9.01-15881, Q:29.01-17111], answer Inspection Methods (RBPS Metric 3.4).
If "Yes" is answered to [Q:9.01-15875, Q:29.01-17110], answer Inbound Vehicle Inspections (RBPS Metric 3.4) related questions.
If "Yes" is answered to [Q:9.01-15882, Q:29.01-17112], answer Outbound Vehicle Inspections (RBPS Metric 3.4) related questions.
If "Yes" is answered to [Q:9.01-15881, Q:29.01-17111], answer Inbound Item Inspections (RBPS Metric 3.4) related questions.
If "Yes" is answered to [Q:9.01-15884, Q:29.01-17113], answer Outbound Item Inspections (RBPS Metric 3.4) related questions.
Once completed, go to Identification Verification System (RBPS Metric 3.1)

Inspection Methods (RBPS Metric 3.4)

Select "Yes" for all the inspection methods that the facility uses.

Inspection Methods [Q:9.02-15888, Q:29.02-17114]	**Yes**	**No**
Visual inspection only	○	○
Use of canines (trained dogs)	○	○
Under Vehicle Lighting System	○	○
CCTV Under Vehicle Search Systems (UVSS)	○	○

Inspection Methods [Q:9.02-15888, Q:29.02-17114]	**Yes**	**No**
Over Vehicle Lighting System	○	○
CCTV Over Vehicle Search Systems (OVSS)	○	○
Cargo and Vehicle Inspection Systems	○	○
Mobile Vehicle Inspection Systems (Imaging)	○	○
Fixed / Portable Vehicle X-Ray Inspection Systems (Imaging)	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.02-15913, Q:29.02-17115]

Inbound Vehicle Inspections (RBPS Metric 3.4)

What method type is used to inspect inbound employee vehicles (POV)?
[Q:9.03-15963, Q:29.03-17116]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.03-16192, Q:29.03-17117]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect inbound company vehicles?
[Q:9.03-16199, Q:29.03-17118]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.03-16200, Q:29.03-17119]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect inbound contractor vehicles?
[Q:9.03-16201, Q:29.03-17120]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.03-16202, Q:29.03-17121]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect inbound delivery vehicles?
[Q:9.03-16203, Q:29.03-17122]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.03-16204, Q:29.03-17123]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect inbound visitor vehicles?
[Q:9.03-16205, Q:29.03-17124]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.03-16206, Q:29.03-17125]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

Inbound Truck and Rail Cars (RBPS Metric 3.4)

Select "Yes" for all the inspection methods that the facility uses for inbound truck and rail cars.

Inspection Methods [Q:9.03-16209, Q:29.03-17126]	**Yes**	**No**
Facility inspects trucks and rail cars upon entering the facility.	○	○
Facility inspects trucks and rail cars prior to loading.	○	○
Other	○	○

If “Other” is selected, enter a description. [Q:9.03-16210, Q:29.03-17127]

Outbound Vehicle Inspections (RBPS Metric 3.4)

Are vehicles allowed access into Theft COI areas?
[Q:9.04-18860, Q:29.04-23098]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of the Outbound Vehicle Inspections (RBPS Metric 3.4) related questions.

What method type is used to inspect outbound employee vehicles (POV) from Theft COI Areas?
[Q:9.045-16211, Q:29.045-17128]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.045-16212, Q:29.045-17129]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect outbound company vehicles from Theft COI Areas?
[Q:9.045-16213, Q:29.045-17130]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.045-16214, Q:29.045-17131]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect outbound contractor vehicles from Theft COI Areas?
[Q:9.045-16215, Q:29.045-17132]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.045-16216, Q:29.045-17133]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect outbound delivery vehicles from Theft COI Areas?
[Q:9.045-16217, Q:29.045-17134]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.045-16218, Q:29.045-17135]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method type is used to inspect outbound visitor vehicles from Theft COI Areas?
[Q:9.045-16219, Q:29.045-17136]

- ○ Not allowed on site
- ○ Cursory inspection
- ○ Random inspection
- ○ Not applicable

If "Random inspection" is selected, enter the amount.
[Q:9.045-16220, Q:29.045-17137]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

Inbound Item Inspections (RBPS Metric 3.4)

What method is used to inspect items hand-carried by inbound employees?
[Q:9.05-16197, Q:29.05-17138]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by inbound regular contractors?
[Q:9.05-16221, Q:29.05-17139]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by inbound temporary contractors?
[Q:9.05-16222, Q:29.05-17140]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by inbound visitors?
[Q:9.05-16223, Q:29.05-17141]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

Outbound Item Inspections (RBPS Metric 3.4)

What method is used to inspect items hand-carried by employees outbound from Theft COI Areas?
[Q:9.06-16224, Q:29.06-17142]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by regular contractors outbound from Theft COI Areas?
[Q:9.06-16225, Q:29.06-17143]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by temporary contractors outbound from Theft COI Areas?
[Q:9.06-16226, Q:29.06-17144]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

What method is used to inspect items hand-carried by visitors outbound from Theft COI Areas?
[Q:9.06-16227, Q:29.06-17145]

- ○ No inspection
- ○ <5% random inspection
- ○ >=5% random inspection
- ○ >=15% random inspection
- ○ >=30% random inspection
- ○ >=50% random inspection
- ○ 100% inspection

Identification Verification System (RBPS Metric 3.1)

Select "Yes" for all the general measures that are used to verify the identity of individuals at the facility.

General Identification Methods [Q:9.07-16229, Q:29.07-17146]	**Yes**	**No**
All individuals being admitted to the facility must present a valid identification prior to being admitted to the facility.	○	○
The facility has implemented a contraband screening program to preclude the introduction of weapons, explosives, drugs, etc. into the facility.	○	○
The facility has implemented and maintains a facility personnel identification program/system to identify personnel authorized access into the facility and restricted/secure areas.	○	○
The facility has implemented a vehicle inspection program to preclude the introduction of weapons, explosives, drugs, unauthorized personnel, etc. into the facility.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.07-16230, Q:29.07-17147]

Personnel Access Control (RBPS Metric 3.1)

Select "Yes" for all methods that are used by personnel to gain access to the facility.

Personnel Access Control [Q:9.07-16250, Q:29.07-17148]	**Yes**	**No**
Personnel access into the facility is through a manned/monitored portal(s) or gate(s).	○	○
The personnel access portal/gate can be secured to prevent access.	○	○
Personnel identities are checked/verified against their assigned access credential.	○	○
Facility uses personnel anti-pass back devices (turnstiles) activated by electronic access systems, i.e., badges.	○	○
ID check performed at Facility outer perimeter.	○	○
ID check performed at Facility internal restricted areas.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.07-16251, Q:29.07-17149]

Are badges required at the facility?
[Q:9.07-16252, Q:29.07-17150]

○ Yes
○ No

If "No" is selected, go to Visitor Access (RBPS Metric 3.1).

Control Measures and Badges (RBPS Metric 3.1)

Select "Yes" for all the control measures that are used at the facility.

Control Measures [Q:9.08-16253, Q:29.08-17151]	**Yes**	**No**
Badges are required to be displayed at all times, unless the wearing of the badge represents a safety or operational concern.	○	○
Facility identification credentials are controlled and retrieved from individuals when employment is terminated, access is not needed due to contract termination, or transfer to another facility.	○	○
Badges are under the control of the individual assigned the badge at all times.	○	○
Badges issued are tamper resistant.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.08-16254, Q:29.08-17152]

Control Measures and Badges (RBPS Metric 3.1)

Select "Yes" for all the manners that photo badges are used at the facility.

Photo Badges [Q:9.08-16255, Q:29.08-17153]	**Yes**	**No**
A numbered, photo ID is provided to all individuals authorized routine access into the facility.	○	○
The photo ID badge indicates the area(s) that an individual is authorized to access within the facility.	○	○
Facility does not use photo ID badges.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.08-16256, Q:29.08-17154]

Control Measures and Badges (RBPS Metric 3.1)

Select "Yes" for all the manners that non-photo badges are used at the facility.

Non-Photo Badges [Q:9.08-16257, Q:29.08-17155]	**Yes**	**No**
Visitors and non-routine individuals permitted access into the facility are provided with a numbered, non-photo badge.	○	○
Non-photo badges indicated that the individual is to be escorted.	○	○
Non-photo badges indicate the area(s) within the facility that do not require an escort.	○	○
Non-photo badges should be readily distinguishable from other badges.	○	○
Facility does not use non-photo badges.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.08-16258, Q:29.08-17156]

Types of Badges Used at the Facility by Each Type of Employee or Visitor.

Select *Yes* for all the types of badges used at the facility by each type of employee or visitor.

Type of Badge Used	**Regular Employee** [Q:9.08-18333, Q:29.08-18361]	**Full-time Contractor** [Q:9.08-18334, Q:29.08-18362]	**Temporary Contractor** [Q:9.08-18335, Q:29.08-18363]	**Visitor** [Q:9.08-18336, Q:29.08-18364]	**N/A** [Q:9.08-18337, Q:29.08-18365]
Government issued photo ID	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
Site-specific photo ID.	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
Site-specific photo ID w/electronic access control.	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No

Type of Badge Used	Regular Employee [Q:9.08-18333, Q:29.08-18361]	Full-time Contractor [Q:9.08-18334, Q:29.08-18362]	Temporary Contractor [Q:9.08-18335, Q:29.08-18363]	Visitor [Q:9.08-18336, Q:29.08-18364]	N/A [Q:9.08-18337, Q:29.08-18365]
Non-photo ID	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
Site-specific photo ID w/electronic access control.	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
No ID required	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No

Visitor Access (RBPS Metric 3.1)

Select "Yes" for all the escort policies in place at the facility.

Escort Policies [Q:9.09-16277, Q:29.09-17165]	**Yes**	**No**
Visitors and individuals shall be escorted while within areas of the facility that require them to be escorted.	○	○
Individuals required to be escorted are not permitted access until their escort arrives and takes custody of them.	○	○
Individuals serving as escorts are briefed on their responsibilities as an escort.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.09-16278, Q:29.09-17166]

Does the facility have an access control system (ACS)?
[Q:9.09-16279, Q:29.09-17167]

○ Yes
○ No

If "No" is selected, go to Vehicle Restrictions (RBPS Metric 3.3).

Access Control System Interface (RBPS Metric 3.1)

Select "Yes" for all the ACS interfaces at the facility.

Access Control System Interfaces [Q:9.1-16280, Q:29.1-17168]	**Yes**	**No**
Barcode Reader	○	○
Biometric Readers	○	○
Magnetic Reader	○	○
Mechanical pushbutton lockset	○	○
Numeric Pad, personal access code	○	○
Numeric Pad, common access code	○	○
Proximity Reader	○	○
Smart Card Reader, contact	○	○
Smart Card Reader, contactless	○	○
Token/Fob readers	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.1-16281, Q:29.1-17169]

Where can the ACS be controlled?
[Q:9.1-16332, Q:29.1-17170]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description. [Q:9.1-16333, Q:29.1-17171]

Where can the ACS be administrated?
[Q:9.1-16334, Q:29.1-17172]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description. [Q:9.1-16335, Q:29.1-17173]

Access Control System Interface (RBPS Metric 3.1)

Select "Yes" if the ACS is monitored in the location.

Monitoring Location [Q:9.1-16336, Q:29.1-17174]	**Yes**	**No**
Local, at the facility	○	○
Another company facility	○	○
Remote, by third-party	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.1-16337, Q:29.1-17175]

Vehicle Restrictions (RBPS Metric 3.3)

Select "Yes" for all the vehicle access restrictions at the facility.

Vehicle Access Restrictions [Q:9.11-16283, Q:29.11-17176]	**Yes**	**No**
Vehicle access into the facility is through a manned or monitored gate(s).	○	○

Vehicle Access Restrictions [Q:9.11-16283, Q:29.11-17176]	**Yes**	**No**
The vehicle gate can be secured to prevent access by a vehicle.	○	○
Only authorized vehicles are permitted to access the facility through the gate.	○	○
Rejection lane prior to site access.	○	○
Vehicle sally port gate entrance for delivery vehicles.	○	○
Separate access gate for contractor personnel.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.11-16284, Q:29.11-17177]

Select "Yes" for all the vehicle identification measures at the facility.

Vehicle Identification [Q:9.11-16285, Q:29.11-17178]	**Yes**	**No**
Vehicle identification program	○	○
Radio Frequency ID (RFID) vehicle tag and reader system	○	○
License plate recognition system	○	○
Known and approved shippers	○	○
Valid bill of lading for delivery to the facility is presented	○	○
Site-issued vehicle ID system	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.11-16286, Q:29.11-17179]

Select "Yes" for all the traffic calming/speed reduction measures used at the facility.

Traffic Calming [Q:9.11-16287, Q:29.11-17180]	**Yes**	**No**
Serpentine traffic pattern/barriers	○	○
Traffic circle	○	○
Speed humps or tables	○	○
Barrier arms/gates, movable	○	○
Bollards, movable	○	○
Wedge barrier, movable	○	○
Traffic control island with vehicle barriers	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.11-16288, Q:29.11-17181]

Parking Restrictions (RBPS Metric 3.3)

Select "Yes" for all the employee parking restrictions at the facility.

Employee Parking Restrictions [Q:9.12-16292, Q:29.12-17182]	**Yes**	**No**
Personally Owned Vehicles (POVs) allowed to park inside the perimeter fence.	○	○
Some POVs allowed to park inside the perimeter fence.	○	○
No POVs are allowed inside the perimeter fence.	○	○
Only "Company-authorized" vehicles are allowed inside the perimeter fence.	○	○
POVs are allowed in designated parking areas outside the perimeter fence.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.12-16297, Q:29.12-17183]

Select "Yes" for all the contractor parking restrictions at the facility.

Contractor Parking Restrictions [Q:9.12-16298, Q:29.12-17184]	**Yes**	**No**
Personally Owned Vehicles (POVs) allowed to park inside the perimeter fence.	○	○
Some POVs allowed to park inside the perimeter fence.	○	○
No POVs are allowed inside the perimeter fence.	○	○
Only "Company-authorized" vehicles are allowed inside the perimeter fence.	○	○
POVs are allowed in designated parking areas outside the perimeter fence.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.12-16299, Q:29.12-17185]

Select "Yes" for all the delivery parking restrictions at the facility.

Delivery Parking Restrictions [Q:9.12-16317, Q:29.12-17186]	**Yes**	**No**
Delivery vehicles may park inside the perimeter fence.	○	○
Some delivery vehicles may park inside the perimeter fence.	○	○
No delivery vehicles may park on site without an escort.	○	○
Delivery vehicles are staged in a secure area outside the perimeter fence.	○	○
Delivery vehicles are staged in a secure area inside the perimeter fence.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.12-16319, Q:29.12-17187]

Select "Yes" for all the visitor parking restrictions at the facility.

Visitor Parking Restrictions [Q:9.12-16328, Q:29.12-17188]	**Yes**	**No**
Personally Owned Vehicles (POVs) allowed to park inside the perimeter fence.	○	○
Some POVs allowed to park inside the perimeter fence.	○	○
No POVs are allowed inside the perimeter fence.	○	○
Only "Company-authorized" vehicles are allowed inside the perimeter fence.	○	○
POVs are allowed in designated parking areas outside the perimeter fence.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:9.12-16329, Q:29.12-17189]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:9.88-15196, Q:29.88-17192]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:9.89-15201, Q:29.89-17193]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 4 – Detect, Deter, and Delay

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 4?
[Q:10.0-18664]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 4.

Anti-Vehicle (RBPS Metric 4.2)

Anti-Vehicle Measure	What is the DOS K Rating on the anti-vehicle measure? [Q:10.015-18856] (Choose One: Not Applicable, DOS K Rating 0, DOS K Rating 4, DOS K Rating 8, DOS K Rating 12, Other, Unknown)	Does the measure have a backup power supply? [Q:10.015-18857]		
		Yes	No	Not Applicable
Berm		○	○	○
Anti-vehicle cable		○	○	○
Beam		○	○	○
Bollard		○	○	○
Cable-beam / Cantilever		○	○	○
Drop arm		○	○	○
K-rail		○	○	○
Embankment		○	○	○
Jersey barrier		○	○	○
Wedge		○	○	○
Vehicle capture net		○	○	○
Case-hardened chains and locks		○	○	○
Planter		○	○	○
Chain link gate reinforcement		○	○	○
Cable barriers		○	○	○
Drum and cable barriers		○	○	○
Dragnet		○	○	○

Anti-Vehicle Measure	What is the DOS K Rating on the anti-vehicle measure? [Q:10.015-18856] (Choose One: Not Applicable, DOS K Rating 0, DOS K Rating 4, DOS K Rating 8, DOS K Rating 12, Other, Unknown)	Does the measure have a backup power supply? [Q:10.015-18857]		
		Yes	No	Not Applicable
Removable nuisance barrier		○	○	○
Guardrail		○	○	○
Motorized barricade		○	○	○
Hydraulic barricade		○	○	○
Electronic barrier gate		○	○	○
Tire-penetrating traffic barrier (One way tire trendles)		○	○	○
Portable roadblock tire-puncturing device		○	○	○
Other		○	○	○

If "Other" is selected, enter a description of the "Other" measure: [Q:10.015-18859]

Traffic Calming/Speed Reduction (RBPS Metric 4.2)

What is the DOS K Rating on the traffic calming/speed reduction measure? [Q:10.02-15241]

Traffic Calming Measure	DOS K Rating (Choose One: Not Applicable, DOS K Rating 0, DOS K Rating 4, DOS K Rating 8, DOS K Rating 12, Other, Unknown)
Serpentine traffic pattern/barriers	
Traffic circle	
Speed humps or tables	
Barrier arms/gates, movable	
Bollards, movable	
Wedge barrier, movable	
Traffic control island with vehicle barriers	
Other	

If "Other" is selected, enter a description of the "Other" measure: [Q:10.02-15242]

Security Lighting (RBPS Metric 4.1)

Does the facility provide and maintain sufficient illumination levels to permit security and facility personnel to safely perform their duties and permit the surveillance of the facility? [Q:10.05-15251]

- ○ Yes
- ○ Partial
- ○ No

If "No" is selected, go to Stationary Posts (RBPS Metric 4.1 and 4.4)

Security Lighting (RBPS Metric 4.1)

Does the security lighting have a backup power supply? [Q:10.06-15252]

- ○ Yes
- ○ No

Lighting Area	Indicate the brightness of the security area. [Q:10.07-15256]	Indicate lighting units. [Q:10.07-22780] (Choose Lumens or Foot-candles)
The facility provides and maintains sufficient illumination levels to permit security and facility personnel to safely perform their duties and permit the surveillance of the facility.		
General street lighting		
Site perimeter lighting		
Security-specific lighting		
Operational lighting		
Portable lighting		
Security gates lighting		
Critical locations lighting		
Other		

If "Other" is selected, enter a description: [Q:10.06-15254]

What percentage of the security gates are covered? [Q:10.07-16268]

Only answer this question if "Security Gates Lighting" is one of the selections for question [Q:10.07-15256], "Indicate the brightness of the security area"

What percentage of the critical locations are covered? [Q:10.07-16270]

Only answer this question if "Critical Locations Lighting" is one of the selections for question [Q:10.07-15256], "Indicate the brightness of the security area"

Stationary Posts (RBPS Metric 4.1 and 4.4)

Select "Yes" for all the stationary posts present at the facility: [Q:10.08-15279]

Stationary Post	Yes	No
Security command center	○	○
Main personnel entrance	○	○
Main vehicle gate	○	○
Roving patrols	○	○
Special posts	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.08-22776]

Structure (RBPS Metric 4.4)

Does the facility have security structures? [Q:10.09-15281]

○ Yes

○ No

If "No" is selected, go to Controls (RBPS Metric 4.4)

Structure (RBPS Metric 4.4)

Enter "Yes" for the choices that are applicable to the facility: [Q:10.1-15282]

Structure Classification	Yes	No
Security structures are provided for protection against the elements.	○	○
Security structures are provided with HVAC systems.	○	○
Security structures are provided for defensive purposes.	○	○
Security structures are bullet-resistant.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.1-15283]

Controls (RBPS Metric 4.4)

Controls	Enter "Yes" for the choices that are applicable to the facility: [Q:10.11-15284]		Is there an associated backup power supply with this item? [Q:10.11-15285]	
	Yes	No	Yes	No
Gate/barrier controls are provided within the structure.	○	○	○	○
Wired and wireless communications are provided within the structure.	○	○	○	○
Intrusion detection system workstation.	○	○	○	○
Access control system workstation.	○	○	○	○
Surveillance system workstation.	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:10.11-22782]

Mobile Patrols (RBPS Metric 4.1)

Indicate "Yes" for the type of mobile patrols utilized at the facility: [Q:10.12-15292]

Mobile Post	Yes	No	Not Applicable
Foot patrols	○	○	○
Vehicle patrols	○	○	○
K-9 patrols	○	○	○
Waterborne patrols	○	○	○
Airborne patrols	○	○	○
Other mobile posts	○	○	○

If "Other" is selected, enter a description: [Q:10.12-23040]

Process Controls (General Data Collection - RBPS 4)

What type of process control functions does the facility have? [Q:10.13-15301]

- ○ Both security and operational functions
- ○ Security functions
- ○ Operational functions
- ○ Neither Security nor operational functionality
- ○ Other

If "Other" is selected, enter a description: [Q:10.13-15356]

CCTV (RBPS Metric 4.3)

Does the facility utilize a CCTV system for facility surveillance? [Q:10.17-15348]

- ○ Yes
- ○ No

Mobile Patrols (RBPS Metric 4.1)

Indicate "Yes" for the type of mobile patrols utilized at the facility: [Q:10.12-15292]

Mobile Post	Yes	No	Not Applicable
Foot patrols	○	○	○
Vehicle patrols	○	○	○
K-9 patrols	○	○	○
Waterborne patrols	○	○	○
Airborne patrols	○	○	○
Other mobile posts	○	○	○

If "Other" is selected, enter a description: [Q:10.12-23040]

Process Controls (General Data Collection - RBPS 4)

What type of process control functions does the facility have? [Q:10.13-15301]

- ○ Both security and operational functions
- ○ Security functions
- ○ Operational functions
- ○ Neither Security nor operational functionality
- ○ Other

If "Other" is selected, enter a description: [Q:10.13-15356]

CCTV (RBPS Metric 4.3)

Does the facility utilize a CCTV system for facility surveillance? [Q:10.17-15348]

- ○ Yes
- ○ No

If "No" is selected, go to Adversary Delay (RBPS Metric 4.1)

CCTV (RBPS Metric 4.3)

Does the CCTV system have a backup power supply? [Q:10.18-15359]

- ○ Yes
- ○ No

Does the CCTV system cover the area?: [Q:10.18-15360]

Area	Yes	Partial	No	Not Applicable
The site provides direct and remote surveillance at critical locations identified in the SVA to detect sabotage.	○	○	○	○
Surveillance is provided for loading areas.	○	○	○	○
Surveillance is provided for unloading areas.	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:10.18-15361]

Is the surveillance system integrated with the access control system? [Q:10.18-15362]

- ○ Yes
- ○ No

Is the surveillance system integrated with the intrusion detection system? [Q:10.18-15363]

- ○ Yes
- ○ No

Where can the CCTV system be controlled? [Q:10.18-15366]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:10.18-15367]

Where can the CCTV system be administrated? [Q:10.18-15368]

- ○ Local at the facility
- ○ Another company facility
- ○ Remote by third-party contractor
- ○ Other
- ○ Not Applicable

If "Other" is selected, enter a description: [Q:10.18-15369]

Is the CCTV system monitored here? [Q:10.18-15370]

Location	Yes	Partial	No
Local, at the facility	○	○	○
Another company facility	○	○	○
Remote, by third-party	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:10.18-15371]

What best describes how the CCTV system is staffed and monitored? [Q:10.18-15372]

- ○ System monitoring and control by dedicated control room operator.
- ○ System monitoring an ancillary responsibility of control room operator.
- ○ System monitoring and control by dedicated security force member.
- ○ System monitoring an ancillary responsibility of security force member.
- ○ Other

If "Other" is selected, enter a description: [Q:10.18-15373]

CCTV Facility Coverage (RBPS Metric 4.3)

Enter the percent of the perimeter fencing monitored via CCTV. [Q:10.18-15376]

Enter the percent of gates that are monitored via CCTV. [Q:10.18-15377]

Enter the percent of critical locations (loading/unloading areas, storage vessels, etc.) monitored via CCTV. [Q:10.18-15378]

CCTV (RBPS Metric 4.3)

Does the facility use the CCTV feature? [Q:10.19-15379]

Camera Technology	Yes	No
No light level	○	○
Low light level	○	○
Day/night switching	○	○
Color	○	○
Black and white	○	○
Infrared imaging	○	○
Thermal imaging	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.19-15380]

Does the facility use the CCTV feature? [Q:10.19-15381]

Camera Type	Yes	No
Fixed view	○	○
Pan-tilt-zoom view	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.19-15382]

Does the facility use the CCTV feature? [Q:10.19-15383]

Camera Communication	Yes	No
Analog/coaxial	○	○
Digital, wired	○	○
Digital, wired with Power Over Ethernet (PoE)	○	○
Digital, wireless	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.19-15384]

Does the facility use the CCTV feature? [Q:10.19-15385]

Camera Controller	Yes	No
Digital recording/controller combination	○	○
Direct camera control	○	○
Matrix switcher	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.19-15386]

Does the facility use the CCTV feature? [Q:10.19-15387]

Recording Medium	Yes	No
Analog/tape	○	○
Digital	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.19-15388]

Adversary Delay (RBPS Metric 4.1)

Does the facility provide additional internal access control and delay barriers to delay an adversary within the facility? [Q:10.2-15389]

○ Yes
○ No
○ Other

If "Other" is selected, enter a description: [Q:10.2-15390]

Locking/Control Devices (RBPS Metric 4.1)

Select "Yes" if the facility has the locking/control device: [Q:10.26-15423]

Locking/Control Device	Yes	Partial	No
Magnetic locks	○	○	○
Gate operators	○	○	○
Electric strike	○	○	○
Movable barrier controllers	○	○	○
Electric lockset	○	○	○
Electrified panic hardware	○	○	○
Electric deadbolt	○	○	○
Locking/control devices have a backup power supply	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:10.26-15424]

Ceiling/Roof (RBPS Metric 4.1)

Does the facility have grilles or other barriers at skylights and louvers over 96 square inches? [Q:10.27-15428]

○ Yes
○ No
○ Other

If "Other" is selected, enter a description: [Q:10.27-15429]

Barrier Upgrades (RBPS Metric 4.1)

Select "Yes" for all the barrier upgrades that the facility utilizes: [Q:10.29-15432]

Locking/Control Device	Yes	Partial	No
Grates placed on culverts inside the facility	○	○	○
Manholes are locked with security fastener/lock	○	○	○
Hardened site openings larger than 96 square inches	○	○	○
Enhanced climb/cut resistant fencing or walls	○	○	○
Foundation enhancements for fencing to prevent tunneling	○	○	○
Burglar-resistant glass	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:10.29-15433]

Key Inventory/Control Program (RBPS Metric 4.1)

Does the facility have a key/lock, combination, and access credential control and accountability program? [Q:10.3-15434]

○ Yes
○ No
○ Other

If "No" is selected, go to Security Force (RBPS Metric 4.5)

If "Other" is selected, enter a description: [Q:10.3-15436]

Key Inventory/Controls (RBPS Metric 4.1)

Select "Yes" for all the key inventory/controls the facility has: [Q:10.31-15439]

Key Inventory/Control	Yes	No
3rd party	○	○
Company	○	○
Security department	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.31-15441]

Control (RBPS Metric 4.1)

Select "Yes" for all the key controls the facility has: [Q:10.31-15442]

Key Control	Yes	No
A log of the issuance of keys, locks, combinations and access credentials is maintained by the facility.	○	○
Keys, locks, combinations, and access credentials are only issues to authorized individual.	○	○
Keys, locks, combinations, and access credentials used at the facility are controlled to reduce possibility of compromise.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.31-15444]

Compromise (RBPS Metric 4.1)

Select "Yes" if the facility follows the procedure: [Q:10.31-15446]

Compromise	Yes	Partial	No
Keys, locks, combinations, and access credentials are changed on a periodic basis.	○	○	○
Keys, locks, combinations, and access credentials are changed when there is suspicion of or they have been compromised.	○	○	○
The key/lock system is re-keyed after a master, core or change key has been lost.	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:10.31-15448]

Inventory (RBPS Metric 4.1)

How frequently (in weeks) is an inventory of keys conducted? [Q:10.31-15451]

How frequently (in weeks) is an inventory of locks conducted? [Q:10.31-18329]

How frequently (in weeks) is an inventory of key and lock combinations conducted? [Q:10.31-18330]

How frequently (in weeks) is an inventory of access credentials conducted? [Q:10.31-18331]

Security Force (RBPS Metric 4.5)

Does the facility have an onsite security force? [Q:10.32-15456]

- ○ Yes
- ○ No

If "No" is selected, go to Posted Personnel (RBPS Metric 4.5)

Security Force (RBPS Metric 4.5)

Does the facility use the security force equipment? [Q:10.33-15457]

Equipment	Yes	No
Uniform	○	○
Radio/wireless communication	○	○
Handcuffs/res	○	○
Baton	○	○
Less-lethal chemical countermeasure (e.g., mace)	○	○
Less-lethal electrical countermeasure (e.g., taser)	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.33-15458]

Does the facility use the security force weapon? [Q:10.33-15459]

Weapons	Yes	No
Revolver	○	○
Automatic pistol/handgun	○	○
Shotgun	○	○
Rifle/long gun	○	○
On-site security force is not armed	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.33-15460]

Security Force Personnel (RBPS Metric 4.5)

Forces On-site

What is the number of unarmed security forces on-site? [Q:10.33-15495]

What is the number of armed security forces on-site? [Q:10.33-15496]

What is the estimated time of first on-site officer to engage adversary (in min)? [Q:10.33-15497]

Forces Off-site

What is the estimated time of the first off-site armed officer to engage adversary (in min)? [Q:10.33-15499]

What is the average response time of additional officers (in min)? [Q:10.33-15501]

Are arrival times tested and documented? [Q:10.33-15466]

- ○ Yes
- ○ No

Posted Personnel (RBPS Metric 4.5)

Are security personnel used to provide surveillance of areas and identify unauthorized activities and/or access to materials? [Q:10.35-15467]

- ○ Yes
- ○ No

Are watchmen used to provide surveillance of areas and identify unauthorized activities and/or access to materials? [Q:10.35-15468]

- ○ Yes
- ○ No

Do the posted personnel provide the observation? [Q:10.35-15469]

Observation	Yes	No
Person(s) provide dedicated observation at a single location.	○	○
Person(s) provide casual observation at a single location.	○	○
Person(s) provide dedicated observation while roving.	○	○
Person(s) provide casual observation while roving.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.35-15470]

Personnel-Based (RBPS Metric 4.5)

Select "Yes" if the facility has this type of site personnel : [Q:10.36-15471]

Personnel Category	Yes	No
Protective forces, dedicated posts/positions	○	○
Protective force, roving patrol	○	○
Operators, dedicated posts/positions	○	○
Operators, roving rounds	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.36-15472]

Tactical Posts (RBPS Metric 4.1 and 4.5)

Select "Yes" if the facility utilizes the post: [Q:10.37-15473]

Tactical Post	Yes	No
Choke points	○	○
Hardened/defensive positions	○	○
Hardened fighting positions	○	○
Defensive positions	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:10.37-15474]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:10.88-15199]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:10.89-15204]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 5 – Shipping, Receiving, and Storage

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 5? [Q:11.0-18674, Q:31.0-18782]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 5
If answering at the Asset level, write the name of the asset for which you are providing answers.

If answering at the Asset level, go to Know Your Customer (RBPS 5.2).

Facility Security Measures

Does the facility have facility-wide security measures for RBPS 5? [Q:11.005-18842]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 5.

Asset Security Measures

Does the facility have asset-specific security measures for RBPS 5 that are different from the facility-wide security measures for RBPS 5? [Q:13.005-17934]

- ○ Yes
- ○ No

Know Your Customer (RBPS 5.2)

Does the facility have a "Know Your Customer" program? [Q:11.01-15286, Q:31.01-16360]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description giving more information: [Q:11.01-15299, Q:31.01-16361]

Does the facility have a Product Stewardship program? [Q:11.01-15287, Q:31.01-16362]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description giving more information: [Q:11.01-15300, Q:31.01-16363]

Shipping, Receiving, and Storage Documentation (General Data Collection RBPS 5 and RBPS Metric 5.5)

What quantity of sales and purchases of hazardous materials (including COI) from manufacturers and distribution of the chemicals of interest are documented? [Q:11.02-15302, Q:31.02-16367]

- ○ All
- ○ Most
- ○ None

What quantity of sales and purchases of hazardous materials (including COI) to 3rd parties are documented? [Q:11.02-15337, Q:31.02-16368]

- ○ All
- ○ Most
- ○ None

Are sales and distribution of hazardous materials (including COI) cross-referenced and provide real-time review of transactions? [Q:11.02-15338, Q:31.02-16369]

- ○ Yes
- ○ No

Does the facility have a procedure ensuring duplicate review and validation of shipping, receiving, and delivery documents for hazardous materials (including COI)? [Q:11.02-15341, Q:31.02-16371]

- ○ Yes
- ○ No

Enter any other information: [Q:11.02-15342, Q:31.02-16372]

Confirmation of Shipments (RBPS Metric 5.4)

What number of shipments of feed material or products to or from the facility does the facility have procedures for confirming before allowing the shipment driver/passengers on-site? [Q:11.03-15345, Q:31.03-16373]

- ○ All
- ○ Most
- ○ None

What number of in-bound and out-bound shipments of hazardous materials (including COI) does the facility conduct advanced planning and approval of? [Q:11.03-15346, Q:31.03-16374]

- ○ All
- ○ Most
- ○ None

Does the facility conduct proper identification checks and verification prior to customer pickup of packaged hazardous materials (including COI)? [Q:11.03-15347, Q:31.03-16375]

- ○ Yes
- ○ No
- ○ Not applicable

Photo Badge Access (General Data Collection - RBPS 5)

Is a numbered photo ID provided to all individuals authorized routine access into the facility? [Q:11.04-15355, Q:31.04-16380]

- ○ Yes
- ○ No

If "No" is selected, go to Carrier (RBPS Metric 5.4)

Does the photo ID badge indicate the area(s) that an individual is authorized to access within the facility? [Q:11.05-15391, Q:31.05-16381]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description of the photo ID badge: [Q:11.05-15392, Q:31.05-16382]

Carrier (RBPS Metric 5.4)

Are all shipments planned and approved in advance using known, approved, carriers? [Q:11.06-15397, Q:31.06-16383]

- ○ Yes
- ○ No

Have approved carriers implemented security measures to provide protection of the vehicle and materials being transported by the carrier? [Q:11.06-15398, Q:31.06-16384]

- ○ Yes
- ○ No

Are security surveys conducted by carriers to ensure compliance and effectiveness of security and protection measures? [Q:11.06-15399, Q:31.06-16385]

- ○ Yes
- ○ No

Are materials that are stored en route stored in secure facilities? [Q:11.06-15400, Q:31.06-16386]

- ○ Yes
- ○ No

Are systems in place to track or protect shipments en route to their destinations, such as drive call-in schedules, GPS tracking, etc.? [Q:11.06-15401, Q:31.06-16387]

- ○ Yes
- ○ No

Enter any other information: [Q:11.06-15402, Q:31.06-16388]

Security: Man-Portable Containers (RBPS Metric 5.1)

What number of hazardous materials (including COI) in man-portable containers have been identified and provided additional protection, such as being chained and locked or otherwise affixed to larger immobile objects or special security tie-downs? [Q:11.07-15403, Q:31.07-16390]

- ○ All
- ○ Most
- ○ None

If "None" is selected, go to Inventory Controls - Purchases/Sales (RBPS Metric 5.2, 5.4, and 5.5)

Select "Yes" for all the man-portable security measures in use at the facility.

Man-Portable Container Security Measure [Q:11.08-15407, Q:31.08-16391]	**Yes**	**No**
The facility has a physical means of securing man-portable containers of hazardous materials (including COI).	○	○
Facility uses a locked rack or other tamper-evident, physical means of securing man-portable containers of Theft COI such as movement alarms on containers, entry/motion detectors and alarms for buildings or rooms where the containers are stored.	○	○
Facility stores hazardous materials (including COI) in large (50kg) bags to increase difficulty of transportation and theft.	○	○
Facility attaches portable containers of hazardous materials (including COI) to larger immobile objects.	○	○
Other	○	○

If "Other" is selected, enter a description of the protection measure. [Q:11.08-15502, Q:31.08-16392]

Inventory Controls - Purchases/Sales (RBPS Metric 5.2, 5.4, and 5.5)

Select "Yes" for all procedures that are in place to control activities related to the purchase and sale of hazardous materials (including COI).

Procedure [Q:11.09-15503, Q:31.09-16393]	**Yes**	**No**
The facility has a procedure to refuse the sale of hazardous materials (including COI) unless consumers produce identification and retailers keep accurate records of transactions. The facility verifies and/or evaluates customer's on-site security.	○	○
The facility has a procedure to review all shipping, receiving and delivery of hazardous materials (including COI).	○	○
Facility has a shipment confirmation program that includes advance planning and approval for receiving and delivering of hazardous materials (including COI).	○	○
Other	○	○

If "Other" is selected, enter a description of the procedure. [Q:11.09-15628, Q:31.09-16394]

Select "Yes" for all procedures that are in place to control activities related to the purchase and sale of hazardous materials (including COI).

Procedure [Q:11.1-15570, Q:31.1-16395]	**Yes**	**No**
The facility conducts a site visit to the customer's business location.	○	○
The facility has a policy to refuse to sell hazardous materials (including COI) to customers that do not meet established customer qualification criteria.	○	○
The facility verifies and/or evaluates customer's on-site security.	○	○
The facility verifies customer's shipping address is a valid business location.	○	○
The facility ensures material is being delivered to a known, approved individual or entity.	○	○
The facility ensures material is being received from a known, approved individual or entity.	○	○
The facility confirms the customer's financial status.	○	○

Procedure [Q:11.1-15570, Q:31.1-16395]	**Yes**	**No**
The facility establishes normal business-to-business payment terms and methods that will prevent cash sales to customers.	○	○
The facility confirms and verifies that the customer's end use of hazardous materials (including COI) is a valid end use.	○	○
Other	○	○

If "Other" is selected, enter a description of the check. [Q:11.1-15630, Q:31.1-16396]

Inventory Controls - Storage/Monitoring (RBPS Metric 5.1 and General Data Collection RBPS 5)

Select "Yes" for all measures that are in place relating to the storage of hazardous materials (including COI).

Protection Measure [Q:11.11-15573, Q:31.11-16397]	**Yes**	**No**
The facility has separate storage areas for hazardous materials (including COI).	○	○
The facility restricts access to the separate storage areas for hazardous materials (including COI).	○	○
The facility has the ability to know where its hazardous materials (including COI) are located at all times.	○	○
The facility secures hazardous materials (including COI) in transportation containers not incident to transportation (rail cars and truck tankers) by storing containers inside the facility's perimeter fencing and monitoring these containers using measures consistent with their contents.	○	○
The facility has a written policy limiting the on-site inventory of specifically identified hazardous materials (including COI) below threshold quantities.	○	○
Other	○	○

If "Other" is selected, enter a description of the measure. [Q:11.11-15632, Q:31.11-16398]

Select "Yes" for all monitoring features that are in place to monitor hazardous materials (including COI) stored at the facility.

Monitoring Feature [Q:11.12-15580, Q:31.12-16399]	**Yes**	**No**
The facility has a system for identifying and reporting evidence of tampering with hazardous materials (including COI).	○	○
The facility has procedures in place that will assist in preventing the theft or diversion of hazardous materials (including COI) using either force or deception.	○	○
The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials (including COI).	○	○
The facility has process controls on all vessels containing hazardous materials (including COI) that monitor their amount (weight and volume) at the facility.	○	○
The facility has a system for reporting and recording shortages of hazardous materials (including COI).	○	○
The facility uses technical surveillance and detection systems to alert other individuals to the act of theft or unauthorized removal of hazardous materials (including COI).	○	○
The facility tracks the disposal of containers of hazardous materials (including COI) and maintains a record of disposed containers.	○	○
The facility links inventory control records of hazardous materials (including COI) to Material Safety Data Sheets (MSDS).	○	○
Other	○	○

If "Other" is selected, enter a description of the monitoring feature. [Q:11.12-15633, Q:31.12-16400]

Monitoring of Shipping and Receiving Areas (RBPS Metric 5.1)

Is the listed measure in place to monitor facility shipping and receiving areas?

Monitoring Measure [Q:11.13-15635, Q:31.13-16401]	**Yes**	**Partial**	**No**
The facility monitors inbound shipments, conducts package and parcel inspection, and controls access by delivery services, vendors, and other shippers.	○	○	○
The facility uses detection equipment to alert personnel to movement of hazardous materials (including COI) through unauthorized portals.	○	○	○
The facility implements an intrusion-detection system for material storage/access locations for hazardous materials (including COI).	○	○	○
Technical devices (access control, video, etc.), patrols, or systems to prevent the unauthorized appropriation of hazardous materials (including COI).	○	○	○
Holding areas for carriers awaiting loads or staged for unloading are secured when vehicles/area is unattended.	○	○	○
Manifolds and exposed access points to tanks containing flammable, toxic, or reactive chemicals are hardened and access is controlled.	○	○	○
Protection and monitoring systems (patrols or CCTV) are in place to assure the security of rail cars located on-site waiting unloading.	○	○	○
Critical process equipment containing hazardous materials (including COI) is monitored using patrols or CCTV to reduce tampering and sabotage potential.	○	○	○
Personnel monitor critical process equipment containing hazardous materials (including COI) directly via CCTV, patrols, or other method to address the potential for tampering, sabotage, or theft.	○	○	○
Other	○	○	○

If "Other" is selected, enter a description of the monitoring feature.
[Q:11.13-15637, Q:31.13-16402]

Vehicle Inspections (RBPS Metric 5.3 and General Data Collection RBPS 5)

Are secure vaults provided within the vehicle, and are tanker truck keys issued only to authorized drivers? [Q:11.14-15638, Q:31.14-16403]

- ○ Yes
- ○ No

Is vehicle access into the facility through monitored or manned gates? [Q:11.14-15639, Q:31.14-16404]

- ○ Yes
- ○ No

What percent of vehicles are inspected on a random basis, upon egress from the restricted area containing the COI or from the facility? [Q:11.14-15641, Q:31.14-16405]

○ 100%	○ 76-99%	○ 51-75%
○ 26-50%	○ 11-25%	○ 6-10%
○ 1-5%	○ None	

Tamper Evident Devices (RBPS Metric 5.1)

Does the facility have a system for identifying and reporting evidence of tampering with hazardous materials (including COI)? [Q:11.15-15764, Q:31.15-16406]

- ○ Yes
- ○ No

If "No" is selected, go to Tamper Evident Devices (RBPS Metric 5.1)

Select "Yes" for all tamper-evident mechanisms used to identify tampering with hazardous materials (including COI).

Tamper-Evident Mechanism [Q:11.16-15777, Q:31.16-16407]	**Yes**	**No**	**Not Applicable**
The facility uses tamper indication sensors.	○	○	○
The facility uses container and shipping seals.	○	○	○
The facility utilizes tamper-evident devices on hazardous materials (including COI).	○	○	○
The facility utilizes numbered tamper-evident devices on hazardous materials (including COI).	○	○	○
The facility uses anti-cargo theft/tampering devices.	○	○	○
Tank trailers are sealed.	○	○	○

Tamper-Evident Mechanism [Q:11.16-15777, Q:31.16-16407]	**Yes**	**No**	**Not Applicable**
Other	○	○	○

If "Other" was chosen, describe any other tamper-evident mechanisms are used to identify tampering with hazardous materials (including COI): [Q:11.16-17555, Q:31.16-17556]

Does the facility employ tamper-evident seals for vehicle valves that can indicate if a shipment has been tampered with? [Q:11.17-15763, Q:31.17-16408]

○ Yes

○ No

If "Yes", list the types of tamper-evident seals used on valves: [Q:11.17-15788, Q:31.17-16409]

Does the facility employ tamper-evident seals for other appurtenances that can indicate if a shipment has been tampered with? [Q:11.17-15790, Q:31.17-16410]

○ Yes

○ No

If "Yes", list the types of tamper-evident seals used on other appurtenances: [Q:11.17-15781, Q:31.17-16411]

Tamper Evident Devices (RBPS Metric 5.1)

Select "Yes" for all controls that are in place to prevent the theft of hazardous materials (including COI).

Theft Control [Q:11.18-15807, Q:31.18-16412]	**Yes**	**No**
The facility stores hazardous materials (including COI) in (a) safe location(s), inside security enclosures, equipped with tamper-resistant locks.	○	○
The facility stores hazardous materials (including COI) in Security enclosures that are equipped with case-hardened tamper-resistant locks.	○	○
In conjunction with an electronic surveillance system, the facility uses security tags, which are attached to or embedded in containers of hazardous materials (including COI) to prevent theft.	○	○
The facility utilizes detection markers, such as chemical additives, to help law enforcement officers identify hazardous materials (including COI).	○	○
The facility uses vehicle alarms.	○	○
The facility uses by-pass or shutdown devices.	○	○
The facility conducts inspections of all vehicles upon egress from the facility or the restricted area for theft of hazardous materials (including COI).	○	○
Other	○	○

If "Other" is selected, enter a description of the theft-prevention measure: [Q:11.18-15857, Q:31.18-16413]

Transportation (RBPS Metric 5.4 and General Data Collection RBPS 5)

Select "Yes" for all items used to maximize transportation security.

Security Measure [Q:11.22-15854, Q:31.22-16421]	**Yes**	**No**
Performance checklists are used that include specific transportation security expectations (e.g., locking vehicle doors, closed windows, key control, safety cones, etc.).	○	○
Teams are used for long trips with hazardous materials (including COI).	○	○
Random checks are conducted on drivers for safety and security activities.	○	○
The facility issues badges to drivers transporting hazardous materials (including COI) pursuant to third party verification of background suitability.	○	○
The facility verifies drivers transporting hazardous materials (including COI) have a proof of suitability, such as a TWIC.	○	○
The facility prevents entry and egress of vehicles at unmanned gates.	○	○
Redundant communication technologies (e.g., radio, satellite phone, etc.) are used during transportation.	○	○
Vehicle theft-protection devices are used to disable fuel, hydraulics, and/or electrical systems.	○	○
Steering columns are locked when tractor is not in service.	○	○
Other	○	○

If "Other" is selected, enter a description of the transportation security measure:
[Q:11.22-15855, Q:31.22-16422]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:11.88-15197, Q:31.88-16427]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:11.89-15202, Q:31.89-16428]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 6 – Theft and Diversion

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 6? [Q:12.0-18677, Q:32.0-18784]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 6.
If answering at the Asset level, write the name of the asset for which you are providing answers.

If answering at the Asset level, go to Shipping, Receiving, and Storage Documentation (RBPS Metric 6.2 and General Data Collection - RBPS 6)

Facility Security Measures

Does the facility have facility-wide security measures for RBPS 6? [Q:12.005-18874]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 6.

Asset Security Measures

Does the facility have asset-specific security measures for RBPS 6 that are different from the facility-wide security measures for RBPS 6? [Q:12.005-17935]

- ○ Yes
- ○ No

Shipping, Receiving, and Storage Documentation (RBPS Metric 6.2 and General Data Collection - RBPS 6)

What quantity of sales and purchases of potentially dangerous chemicals (including Theft COI) are documented? [Q:12.01-15915, Q:32.01-16957]

- ○ All
- ○ Most
- ○ None

What quantity of sales and purchases of potentially dangerous chemicals (including Theft COI) to 3rd parties are documented? [Q:12.01-15916, Q:32.01-16958]

- ○ All
- ○ Most
- ○ None

Are sales and distribution of potentially dangerous chemicals (including Theft COI) cross-referenced and provide real-time review of transactions? [Q:12.01-15917, Q:32.01-16959]

- ○ Yes
- ○ No

Does the facility have a procedure for the review and validation of shipping, receiving, and delivery documents for potentially dangerous chemicals (including Theft COI)? [Q:12.01-15918, Q:32.01-16960]

- ○ Yes
- ○ No

Enter any other information: [Q:12.01-15922, Q:32.01-16962]

Access Control (RBPS Metric 6.1)

Does the facility have controls and procedures that restrict access to storage of potentially dangerous chemicals (including Theft COI), allowing access only to authorized individuals? [Q:12.03-15934, Q:32.03-16974]

- ○ Yes
- ○ No

Are transportation access portals controlled and is access limited to authorized individuals? [Q:12.03-15935, Q:32.03-16975]

- ○ Yes
- ○ No

Enter any other information: [Q:12.03-15936, Q:32.03-16976]

Photo Badge Access (RBPS Metric 6.1)

Is a numbered photo ID provided to all individuals authorized routine access into the facility? [Q:12.04-15938, Q:32.04-16978]

- ○ Yes
- ○ No

If "No" is selected, go to Carrier (General Data Collection - RBPS 6)

Photo Badge Access (RBPS Metric 6.1)

Does the photo ID badge indicate the area(s) that an individual is authorized to access within the facility? [Q:12.05-15940, Q:32.05-16980]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description of the photo ID badge: [Q:12.05-15967, Q:32.05-16981]

Carrier (General Data Collection - RBPS 6)

Are all shipments planned and approved in advance using known, approved, carriers? [Q:12.06-15944, Q:32.06-16986]

- ○ Yes
- ○ No

Unknown Carrier or Driver (General Data Collection - RBPS 6)

Select "Yes" if the facility has procedure in place.

Procedure for … [Q:12.07-15968, Q:32.07-16994]	**Yes**	**No**
Arrival of an unknown carrier or an unknown driver at the facility.	○	○
Staging both driver and the vehicle until both the driver and the load being delivered or being picked up are properly vetted and approved.	○	○
Refusing the load being delivered or being picked up if the driver and carrier are not approved.	○	○

Procedure for … [Q:12.07-15968, Q:32.07-16994]	**Yes**	**No**
Sequestering both vehicle and driver while the facility attempts to approve identity of driver and identity of the load.	○	○
Notifying and contacting local law enforcement depending on the identity of the driver and identity of the load.	○	○
Other	○	○

If "Other" is selected, enter a description of the additional procedure [Q:12.07-16235, Q:32.07-16995]

Security: Man-Portable Containers (RBPS Metric 6.5)

What number of potentially dangerous chemicals (including Theft COI) in man-portable containers have been identified and provided additional protection, such as being chained and locked or otherwise affixed to larger immobile objects or special security tie-downs? [Q:12.08-15969, Q:32.08-17001]

- ○ All
- ○ Most
- ○ None

If "None" is selected, go to Inventory Controls - Purchases/Sales (RBPS Metric 6.8)

Select "Yes" for all measures that are in place for protecting potentially dangerous chemicals (including Theft COI) man-portable assets at the facility.

Protection Measure [Q:12.09-15970, Q:32.09-17002]	**Yes**	**No**
The facility has a physical means of securing man-portable containers of potentially dangerous chemicals (including Theft COI).	○	○
Facility uses a locked rack or other tamper-evident, physical means of securing man-portable containers of potentially dangerous chemicals (including Theft COI) such as movement alarms on containers, entry/motion detectors and alarms for buildings or rooms where the containers are stored.	○	○
Facility stores potentially dangerous chemicals (including Theft COI) in large (50kg) bags to increase difficulty of transportation and theft.	○	○
Facility attaches portable containers of potentially dangerous chemicals (including Theft COI) to larger immobile objects.	○	○
Other	○	○

If "Other" is selected, enter a description of the protection measure: [Q:12.09-15971, Q:32.09-17003]

Inventory Controls - Purchases/Sales (RBPS Metric 6.8)

Select "Yes" for all checks that are in place to control activities related to the purchase and sale of potentially dangerous chemicals (including Theft COI).

Check [Q:12.11-15974, Q:32.11-17009]	**Yes**	**No**
The facility conducts a site visit to the customer's business location.	○	○
The facility has a policy to refuse to sell potentially dangerous chemicals (including Theft COI) to customers that do not meet established customer qualification criteria.	○	○
The facility verifies and/or evaluates customer's on-site security.	○	○
The facility verifies customer's shipping address is a valid business location.	○	○
The facility ensures material is being delivered to a known, approved individual or entity.	○	○
The facility ensures material is being received from a known, approved individual or entity.	○	○
The facility confirms the customer's financial status.	○	○
The facility establishes normal business-to-business payment terms and methods that will prevent cash sales to customers.	○	○
The facility confirms and verifies that the customer's end use of the potentially dangerous chemicals (including Theft COI) is a valid end use.	○	○
Other	○	○

If "Other" is selected, enter a description of the protection measure: [Q:12.11-15975, Q:32.11-17010]

Inventory Controls - Storage/Monitoring (RBPS Metric 6.8)

Select "Yes" for all measures that are in place relating to the storage of potentially dangerous chemicals (including Theft COI).

Measure [Q:12.12-15976, Q:32.12-17014]	**Yes**	**No**
The facility has separate storage areas for potentially dangerous chemicals (including Theft COI).	○	○
The facility restricts access to the separate storage areas for potentially dangerous chemicals (including Theft COI).	○	○
The facility has the ability to know where its potentially dangerous chemicals (including Theft COI) are located at all times.	○	○
The facility secures potentially dangerous chemicals (including Theft COI) in transportation containers not incident to transportation (rail cars and truck tankers) by storing containers inside the facility's perimeter fencing and monitoring these containers using measures consistent with their contents.	○	○
The facility has a written policy limiting the on-site inventory of specifically identified potentially dangerous chemicals (including Theft COI) below threshold quantities.	○	○
The facility has process controls on potentially dangerous chemicals (including Theft COI).	○	○
Other	○	○

If "Other" is selected, enter a description of the measure: [Q:12.12-15977, Q:32.12-17015]

Employee Training to Identify Theft and Diversion (General Data Collection - RBPS 6)

Training Frequency [Q:12.2-16181, Q:32.2-17035]	(Choose one: monthly, quarterly, semi-annually, annually, biennially, triennially, never)
How often does the facility conduct training on recognizing and detecting explosive materials?	
How often does the facility conduct training on recognizing and detecting explosive devices?	

Training Frequency [Q:12.2-16181, Q:32.2-17035]	(Choose one: monthly, quarterly, semi-annually, annually, biennially, triennially, never)
How often does the facility conduct training on recognizing and detecting improvised explosive?	
How often does the facility conduct training on recognizing and detecting hand-carried weapons?	
How often does the facility conduct training on recognizing and detecting Surveillance devices (e.g., camera phones)?	
How often does the facility conduct training on recognizing characteristics and behavioral patterns of persons who are likely to threaten security?	
How often does the facility conduct training on general techniques used to circumvent security measures?	

Does the facility require individuals granted unescorted accesses to the facility to attend security awareness training at the facility? [Q:12.2-16183, Q:32.2-17036]

- ○ Yes
- ○ No

If the facility provides other training related to theft and diversion, please describe:
[Q:12.2-16185, Q:32.2-17037]

Background Investigation (RBPS Metric 6.3)

Select "Yes" for all background investigations that are performed.

Background Investigation [Q:12.22-16191, Q:32.22-17041]	**Yes**	**No**
Employees, contractors, and others requiring unescorted access to the facility and restricted areas within the facility must successfully complete a background suitability check prior to being granted unescorted access to the facility.	○	○
Job applicants complete background investigation forms and sign appropriate release authorizations to be used to conduct a preemployment background investigation.	○	○
Contractors certify that they have an employee background screening program and that the employees working at the facility have successfully passed the screening process.	○	○

Background Investigation [Q:12.22-16191, Q:32.22-17041]	**Yes**	**No**
Other	○	○

If "Other" is selected, enter a description of the background investigation: [Q:12.22-16193, Q:32.22-17042]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:12.88-15181, Q:32.88-16807]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:12.89-15182, Q:32.89-16735]

For more information, refer to the SSP instructions.

RBPS 7 – Sabotage

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 7? [Q:13.0-18678, Q:33.0-18786]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 7
If answering at the Asset level, write the name of the asset for which you are providing answers.

If answering at the Asset level, go to Sabotage Protection (RBPS Metric 7.1 and General Data Collection - RBPS 7)

Facility Security Measures

Does the facility have facility-wide security measures for RBPS 7? [Q:13.004-18875]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 7.

Asset Security Measures

Does the facility have asset-specific security measures for RBPS 7 that are different from the facility-wide security measures for RBPS 7? [Q:13.004-17936]

- ○ Yes
- ○ No

Sabotage Protection (RBPS Metric 7.1 and General Data Collection - RBPS 7)

Does the facility have the following sabotage control measures (check all that apply): [Q:13.005-15987, Q:33.005-16740]

For each checked response, answer the questions that are associated with that category.

☐	Procedures	*Procedures (RBPS Metric 7.1)*
☐	Access Control	*Access Control (RBPS Metric 7.3)*
☐	Communications	*Communications (General Data Collection - RBPS 7)*
☐	2-Person Rule	*2-Person Rule (General Data Collection - RBPS 7)*
☐	Inventory Controls	*Inventory Controls - Purchases/Sales (RBPS Metric 7.1 and General Data Collection - RBPS 7)*
☐	Rail/Tanker Storage	*Rail/Tanker Storage (RBPS Metric 7.2 and RBPS Metric 7.3)*
☐	Labor	*Labor (General Data Collection - RBPS 7)*
☐	Employee Training	*Employee Training to Identify Sabotage (RBPS Metric 7.1)*
☐	Personnel Surety	*Personnel Surety - Sabotage COI (RBPS Metric 7.3)*
☐	Carrier	*Carrier (RBPS Metric 7.1)*
☐	Other	

If "Other" is selected, enter a description: [Q:13.005-15989, Q:33.005-16741]

Procedures (RBPS Metric 7.1)

Please indicate if the facility has the following procedures for sabotage control (check all that apply):

Does the facility has a procedure to conduct routine equipment inspections for tampering? [Q:13.01-15991, Q:33.01-16742]

○ Yes
○ No

Does the facility has a procedure in place to conduct security awareness training? [Q:13.01-15992, Q:33.01-16743]

○ Yes
○ No

Does the facility have a process safety management system in place? [Q:13.01-15993, Q:33.01-16744]

○ Yes
○ No

Does the facility has procedures/protocols in place for verifying the identity and shipment orders of carriers that arrive to remove transportation containers of sabotage COI? [Q:13.01-15994, Q:33.01-16745]

- ○ Yes
- ○ No

If the facility has other procedures that address sabotage, please describe. [Q:13.01-15994, Q:33.01-16746]

Access Control (RBPS Metric 7.3)

Does the facility have controls and procedures that restrict access to storage of Sabotage COI, allowing access only to authorized individuals? [Q:13.02-16261, Q:33.02-16747]

- ○ Yes
- ○ No

Does the facility control transportation access portals and access is limited to authorized individuals? [Q:13.02-16264, Q:33.02-16748]

- ○ Yes
- ○ No

Does the facility provides additional access controls at critical locations to make it highly unlikely that unauthorized personnel or unescorted visitors will gain access? [Q:13.02-16267, Q:33.02-16749]

- ○ Yes
- ○ No

Access Control - Visitors

What type of visitor access does the facility permit? [Q:13.02-16290, Q:33.02-16751]

- ○ The facility has implemented visitor identification, escort, and control procedures.
- ○ The facility has documented and implemented visitor identification, escort, and control procedures.
- ○ The facility has documented and implemented visitor identification, escort, and control procedures that require verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.
- ○ The facility has documented and implemented strict visitor identification, escort, and control procedures that require verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.
- ○ None, the facility does not permit any visitor access.

Does the facility has backup power supply for its access controls? [Q:13.02-16293, Q:33.02-16752]

- ○ Yes
- ○ No

If there are any other access control measures for visitors, please describe. [Q:13.02-16294], Q:33.02-16753]

Communications (General Data Collection - RBPS 7)

Please indicate if the facility has the following communication systems for sabotage control (check all that apply): [Q:13.04-16349, Q:33.04-16757]

- ☐ The facility provides redundant, highly reliable, communication and duress annunciation systems.
- ☐ The facility has reliable, communication and duress annunciation systems.
- ☐ The facility has communication and duress annunciation systems.
- ☐ Facility has backup power supply for the communications systems.
- ☐ Other

If "Other" is selected, enter a description: [Q:13.04-16354, Q:33.04-16758]

2-Person Rule (General Data Collection - RBPS 7)

Does the facility implement a "2-person" rule during highly critical activities subject to potential sabotage? [Q:13.05-16355, Q:33.05-16759]

- ○ Yes
- ○ No

Please describe your response to the above question. [Q:13.05-16356, Q:33.05-16760]

Inventory Controls - Purchases/Sales (RBPS Metric 7.1 and General Data Collection - RBPS 7)

Please indicate if the facility has the following inventory control measures during purchase and sale of Sabotage COI (provide answer for each – even if the answer is no or never) [Q:13.06-16438, Q:33.06-16761]	**Yes**	**No**
The facility has written security procedures and instructions to control activities related to sales and storage of Sabotage COI.	○	○
Facility conducts a site visit to the customer's business location.	○	○
Facility has a procedure to refusing the sale of packaged chemical unless consumers produce identification and retailers keep accurate records of transactions.	○	○
Facility has a policy to refuse to sell Sabotage COI to customers that do not meet established customer qualification criteria.	○	○
Facility verifies and/or evaluates customer's on-site security.	○	○
Facility verifies customer's shipping address is a valid business location.	○	○
Facility has a shipment confirmation program that includes advance planning and approval for receiving and delivering of Sabotage COI.	○	○
Facility has a procedure to review all shipping, receiving and delivery of Sabotage COI.	○	○
Facility ensures material is being delivered to a known, approved individual or entity.	○	○
Facility ensures material is being received from a known, approved individual or entity.	○	○
Facility confirms the customer's financial status.	○	○
Facility establishes normal business-to-business payment terms and methods that will prevent cash sales to customers.	○	○
Facility confirms and verifies that the customer's end use of the Sabotage COI is a valid end use.	○	○
Facility has procedures and detailed instructions needed to control activities related to sales and storage of Sabotage COI.	○	○
Other	○	○

If "Other" is selected, please describe: [Q:13.06-16441, Q:33.06-16762]

Inventory Controls - Procedures (RBPS Metric 7.1 and General Data Collection - RBPS 7)

Please indicate if the facility has the following inventory control procedures for sabotage control (provide answer for each - even if the answer is no or never) [Q:13.07-16442, Q:33.07-16763]	**Yes**	**No**
The facility has written security procedures and instructions to control activities related to sales and storage of Sabotage COI.	○	○
Facility has separate storage areas for Sabotage COI.	○	○
The facility restricts access to the separate storage areas for Sabotage COI.	○	○
Facility has a system for identifying and reporting evidence of tampering with Sabotage COI.	○	○
Facility has ability to know where its Sabotage COI product is located at all times.	○	○
Facility has procedures in place that will assist in preventing the theft or diversion of materials using either force or deception.	○	○
The facility has documented processes for securing and monitoring the shipment, receipt, and storage of Sabotage COI.	○	○
The facility has a written policy limiting the on-site inventory of specifically identified Sabotage COI below threshold quantities.	○	○
Other	○	○

If "Other" is selected, please describe: [Q:13.07-16445, Q:33.07-16764]

Inventory Controls - Storage/Monitoring (RBPS Metric 7.1 and General Data Collection - RBPS 7)

Please indicate if the facility has the following storage and monitoring measures for sabotage control (provide answer for each - even if the answer is no or never) [Q:13.08-16448, Q:33.08-16765]	**Yes**	**No**
Facility secures Sabotage COI containing transportation containers not incident to transportation (rail cars and truck tankers) by storing containers inside the facility's perimeter fencing and monitoring these containers using measures consistent with Sabotage COI material.	○	○
Facility has process controls on all vessels containing Sabotage COI to monitor amount (weight and volume) of Sabotage COI at the facility.	○	○
Facility has a system for reporting and recording shortages of Sabotage COI.	○	○
Facility uses technical surveillance and detection systems to alert other individuals to the act of theft or unauthorized removal of Sabotage COI.	○	○
The facility has process controls on Sabotage COI.	○	○
Facility tracks the disposal of containers of Sabotage COI and maintains a record of disposed containers.	○	○
Facility links inventory control records of Theft COI and other dangerous chemicals to Material Safety Data Sheets (MSDS).	○	○
Other	○	○

If "Other" is selected, please describe: [Q:13.08-16450, Q:33.08-16766]

Rail/Tanker Storage (RBPS Metric 7.2 and RBPS Metric 7.3)

Please indicate if the facility has the following rail/tanker storage measures for sabotage control (check all that apply) [Q:13.09-16454, Q:33.09-16767]

- ☐ The facility provides secure railcar and tanker truck staging areas.
- ☐ The facility provides secure railcar and tanker truck staging areas where it is unlikely that unauthorized individuals could gain access.
- ☐ The facility provides secure railcar and tanker truck staging areas where it is highly unlikely that unauthorized individuals could gain access.
- ☐ Other

If "Other" is selected, please describe: [Q:13.09-16462, Q:33.09-16768]

Labor (General Data Collection - RBPS 7)

Does the facility have programs that foster good communication between management and the workforce to reduce workplace violence and potential sabotage? [Q:13.1-16464, Q:33.1-16769]

- ○ Yes
- ○ No
- ○ Other

Please describe your answer to the above question. [Q:13.1-16466, Q:33.1-16770]

Employee Training to Identify Sabotage (RBPS Metric 7.1)

Does the facility conducts training on recognition and detection of dangerous substances and devices (provide answer for each - even if the answer is no or never): [Q:13.11-16482, Q:33.11-16771]

Please select the training frequency (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)

How often does the facility conduct training on recognizing and detecting explosive materials?	
How often does the facility conduct training on recognizing and detecting explosive devices?	

Does the facility conducts training on recognition and detection of dangerous substances and devices (provide answer for each - even if the answer is no or never): [Q:13.11-16482, Q:33.11-16771]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
How often does the facility conduct training on recognizing and detecting improvised explosive?	
How often does the facility conduct training on recognizing and detecting hand-carried weapons?	
How often does the facility conduct training on recognizing and detecting Surveillance devices (e.g., camera phones)?	
How often does the facility conduct training on recognizing characteristics and behavioral patterns of persons who are likely to threaten security?	
How often does the facility conduct training on general techniques used to circumvent security measures?	

Does the facility require individuals granted unescorted accesses to the facility to attend security awareness training at the facility? [Q:13.11-16488, Q:33.11-16772]

- ○ Yes
- ○ No

If the facility provides other training related to sabotage, please describe: [Q:13.11-16490, Q:33.11-16773]

Personnel Surety - Sabotage COI (RBPS Metric 7.3)

How does the facility make a "suitability determination" for employees with access to Sabotage COI? [Q:13.12-16497, Q:33.12-16774]

- ○ The facility does not make a "suitability determination"
- ○ Facility makes a "suitability determination" by conduction pre-employment checks on employees with access to Sabotage COI.
- ○ Facility makes a "suitability determination" by conducting background investigations on employees with access to Sabotage COI.
- ○ Facility makes a "suitability determination" without conducting background investigations on employees with access to Sabotage COI.
- ○ Other

If "Other" is selected, please describe. [Q:13.12-16498, Q:33.12-16775]

Carrier (RBPS Metric 7.1)

Please indicate if the facility has the following checks on carriers transporting sabotage COI (provide answer for each - even if the answer is no or never): [Q:13.13-16501, Q:33.13-16776]	**Yes**	**No**
All shipments are planned and approved in advance using known, approved, carriers.	○	○
Approved carriers have implemented security measures to provide protection of the vehicle and materials being transported by the carrier.	○	○
Security surveys are conducted by carriers to ensure compliance and effectiveness of security and protection measures.	○	○
Materials stored en route during transportation are stored in secure facilities.	○	○
Systems are in place to track or protect shipments en route to their destinations, such as drive call-in schedules, GPS tracking, etc.	○	○
Other	○	○

If "Other" is selected, please describe. [Q:13.13-16504, Q:33.13-16777]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:13.88-15198, Q:33.88-17199]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:13.89-15203, Q:33.89-17200]

For more information, refer to the SSP instructions.

RBPS 8 – Cyber Security

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 8? [Q:14.0-18679]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 8.

Policies and Procedures (RBPS Metric 8.1.1, 8.9, 8.3.4)

Does the facility develop and maintain cyber security policies and procedures? [Q:14.01-15494]

- ○ Yes
- ○ No

If "No" is selected, go to IT Personnel (RBPS Metric 8.1.2, 8.3.2).

Procedures (RBPS Metric 8.1.1

Which option best describes the facility's approach to insure the cyber security documentation commensurate with the facility's current information technology operating environment? (Check one) [Q:14.02-15294]

- ○ The facility has documented and distributed cyber security policies, plans and supporting procedures.
- ○ The facility has (at a minimum) documented and distributed cyber security policies or plans.
- ○ The facility incorporates security controls.
- ○ Other

If "Other" is selected, enter a description for the cyber security approach. [Q:14.02-15304]

Security Procedures (RBPS Metric 8.1.1)

Which option best describes the facility's approach for the cyber change management policy (e.g., new hardware/software, employee access)? (Check one) [Q:14.02-15343]

- ○ The facility has a documented and distributed cyber change management policy and supporting procedures.
- ○ The facility has documented and distributed change management procedures.
- ○ The facility has audit logs documenting who made the changes to a policy, plan, and procedures and date of those changes.
- ○ Other

If "Other" is selected, enter a description for the option. [Q:14.02-15412]

Audits (RBPS Metric 8.9)

How often does the facility conduct audits that measure compliance with the facility's cyber security policies, plans, and procedures and those results must be reported to senior management? (Check one) [Q:14.02-15427]

- ○ Annual audits
- ○ Triennial audits
- ○ Other

If "Other" is selected, enter a description for the type of the audit. [Q:14.02-15440]

Third Party Cyber Support (RBPS Metric 8.3.4)

Does the facility ensure that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for facility employees? [Q:14.02-15443]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the type of the control measures.
[Q:14.02-15452]

IT Personnel (RBPS Metric 8.1.2, 8.3.2)

Does the facility employ an individual(s) responsible for information technology network for the facility? [Q:14.1-15465]

- ○ Yes
- ○ No

If "No" is selected, go to Network Accounts and Access (RBPS Metric 8.2.1 - 8.2.5, 8.3.1, 8.3.3).

Officials (RBPS Metric 8.1.2)

Has the facility designated an individual(s) to manage cyber security for the facility that can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop and implement the company's cyber security policies and procedures, and ensure compliance with all applicable industry and governmental cyber security requirements? [Q:14.11-15475]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the type of the specific cyber security personnel solution. [Q:14.11-15477]

Separation of Duties (RBPS Metric 8.3.2)

Are systems administration and IT security duties performed by different individuals?
[Q:14.11-15482]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the specific policy for the separation of duties. [Q:14.11-15510]

Network Accounts and Access (RBPS Metric 8.2.1 - 8.2.5, 8.3.1, 8.3.3)

Does the facility maintain accounts and access controls for the facility IT network? [Q:14.2-15557]

- ○ Yes
- ○ No

If "No" is selected, go to Cyber Security Training (RBPS Metric 8.4.1).

Unique Accounts (RBPS Metric 8.3.1)

Where users function as a group (e.g., control system operators) and user identification and authentication may be role based, does the Facility implement appropriate compensating security controls (e.g., physical controls)? [Q:14.21-15604]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the access account management system. [Q:14.21-15605]

Criticality Sensitivity Review (RBPS Metric 8.3.1)

Does the facility review and establish security requirements for positions that permit administrative access to systems? [Q:14.21-15606]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the criticality sensitivity review. [Q:14.21-15607]

Password Management (RBPS Metric 8.2.5)

The facility implements the following password management policy: [Q:14.21-15610] **Indicate "Yes" for the password management policy that apply.**	**Yes**	**No**
Facility ensures that all default passwords have been changed.	○	○
Facility documents and enforces password structures for administrative and user accounts.	○	○
Facility implements appropriate physical controls for cyber systems where changing default passwords is not technically feasible (e.g., control system with hard-coded password).	○	○
Other	○	○

If "Physical Controls", enter a description for the controls. [Q:14.21-15615]

If "Other" is selected, enter a description for the password management policy. [Q:14.21-15616]

Physical Access to Cyber Systems and Information Storage (RBPS Metric 8.3.5)

Does the facility have role-based physical access controls to restrict access to critical cyber assets and media? [Q:14.21-15617]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the physical access controls. [Q:14.21-15618]

Least Privilege (RBPS Metric 8.2.3)

Does the facility practice the concept of least privilege (i.e., users are only granted access to those information, files, and applications based on role and responsibilities)? [Q:14.21-15619]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the least privilege concept. [Q:14.21-15620]

Access Control Lists (RBPS Metric 8.3.3)

Does the facility maintain access control lists, and ensures that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated? (Check all that apply) [Q:14.21-15862]

- ☐ By close of business the day personnel leave the company under adverse action
- ☐ Within one business day of personnel leaving the company or transferring into new roles
- ☐ Within one week of personnel leaving the company or transferring into new roles
- ☐ Other

If "Other" is selected, enter a description for the access controls. [Q:14.21-15863]

External Connections (RBPS Metric 8.2.2)

The facility maintains external connections requirements: [Q:14.21-15610] **Indicate "Yes" for the external connections requirement that apply.**	**Yes**	**No**
Facility has established and documented a business requirement for every external connection to/from their systems and networks.	○	○
Facility may allow external connections to systems if controls only permit authorized and authenticated user access.	○	○
Other	○	○

If "Other" is selected, enter a description for the external connections requirements. [Q:14.21-15865]

System Boundaries (RBPS Metric 8.2.1)

Does the facility identify and document systems boundaries (i.e., the electronic perimeter) and implements security controls to limit access across those boundaries? [Q:14.21-15866]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the system boundaries. [Q:14.21-15867]

Access Controls Rules of Behavior (RBPS Metric 8.2.4)

Does the facility define allowable remote access and rules of behavior (e.g., Internet, Virtual private network (VPN), gateways, routers, firewalls, wireless access points, modems, vendor maintenance connections, Internet Protocol (IP) address ranges)?
[Q:14.21-15868]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the access controls rules of behavior.
[Q:14.21-15869]

Cyber Security Training (RBPS Metric 8.4.1)

Does the facility provide cyber security training for its employees? [Q:14.3-15873]

- ○ Yes
- ○ No

If "No" is selected, go to Network Monitoring and Incident Reporting (RBPS Metric 8.5.1-8.5.5, 8.6).

When does the facility provide cyber security training to all new employees that work with critical cyber assets or systems? [Q:14.31-15904]

- ○ Before obtaining access
- ○ Within 30 days of obtaining access
- ○ Other

If "Other" is selected, enter a description for the cyber security training timing.
[Q:14.31-15909]

Cyber Security Training Process

The facility has established the following cyber security training process: [Q:14.31-15912] **Indicate "Yes" for the cyber security training process.**	**Yes**	**No**
All employees who work with critical cyber assets or systems receive cyber security awareness training on an annual basis.	○	○
All cyber security training is applicable to the level of the employee's responsibilities.	○	○
All employees are trained in the general cyber security topics.	○	○
Other	○	○

If "Other" is selected, enter a description for the cyber security training process. [Q:14.31-15919]

If "No" is answered to "All employees are trained in the general cyber security topics" in [Q:14.31-15912], go to Cyber Training Instructions.

Cyber Security Topics (RBPS Metric 8.4.1)

The facility provides training to all employees in the following general cyber security topics: [Q:14.32-15962]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
General company policy review	
Roles and responsibilities	
Password procedures	
Acceptable practices	
Whom to contact and how to report suspected inappropriate or suspicious activity	
Other	

If "Other" is selected, enter a description for the cyber security training method.
[Q:14.32-15962]

Cyber Training Instructions

Does the facility have a role-based cyber security training program for its employees?
[Q:14.31-15933]

- ○ Yes
- ○ No

If "No" is selected, go to Network Monitoring and Incident Reporting (RBPS Metric 8.5.1-8.5.5, 8.6).

Cyber Security Instructional Methods (RBPS Metric 8.4.1)

The following Cyber Training Instructional Methods are used: [Q:14.32-15965] **Indicate "Yes" for the cyber training instructional method that apply.**	**Yes**	**No**
Hands-on activities	○	○
Hand-outs, bulletin boards, etc	○	○
Lectures	○	○
On-line or interactive programs	○	○
Orientations	○	○
Seminars	○	○
Workshops	○	○
Briefings	○	○
Video	○	○
Other	○	○

If "Other" is selected, enter a description for the cyber security training instructional method. [Q:14.32-15966]

Network Monitoring and Incident Reporting (RBPS Metric 8.5.1-8.5.5, 8.6)

Does the facility have remote access to process control systems? [Q:14.4-16036]

- ○ Yes
- ○ No

Is the system protected by cyber security controls to prevent intrusion or remote access? [Q:14.4-16053]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:14.4-16036], answer the following: Network Monitoring (RBPS Metric 8.5.2), Network Monitoring Log (RBPS Metric 8.5.2), Network Monitoring SIS (RBPS Metric 8.5.5), and Cyber Security (RBPS Metric 8.5.1).

If "Yes" is selected for [Q:14.4-16053], answer the following: Incident Response (RBPS Metric 8.5.3), Incident Reporting (RBPS Metric 8.5.4), Post-Incident Measures (RBPS Metric 8.6)

Network Monitoring (RBPS Metric 8.5.2)

Does the facility have the capability to monitor networks in real-time with immediate alerts? [Q:14.41-16124]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the network monitoring method. [Q:14.41-16139]

Network Monitoring Log (RBPS Metric 8.5.2)

What is the review frequency for the cyber-security event log? (Check one) [Q:14.41-16160]

- ○ Reviewed daily
- ○ Reviewed at least weekly
- ○ Other

If "Other" is selected, enter a description for the log review frequency. [Q:14.41-16166]

Network Monitoring SIS (RBPS Metric 8.5.5)

The facility control systems with Safety Instrumented Systems have configured the Safety Instrumented Systems such that they have no unsecured remote access and: [Q:14.41-16171] **Indicate "Yes" for the Safety Instrumented Systems configuration that apply.**	**Yes**	**No**
No direct connections to the systems managing the processes they monitor.	○	○
No unsecured direct connections to the systems managing the processes they monitor.	○	○
Other	○	○

If "Other" is selected, enter a description for the Safety Instrumented Systems configuration. [Q:14.41-16180]

Cyber Security (RBPS Metric 8.5.1)

The facility maintains the following cyber security approach: [Q:14.41-16190] **Indicate "Yes" for the cyber security approach that apply.**	**Yes**	**No**
Facility ensures that cyber security controls are in place to prevent malicious code from exploiting critical cyber systems.	○	○

The facility maintains the following cyber security approach: [Q:14.41-16190] **Indicate "Yes" for the cyber security approach that apply.**	**Yes**	**No**
Facility is aware of available software security patches and updates and applies appropriate patches and updates to systems as soon as possible given critical operational and testing requirements.	○	○
Other	○	○

If "Other" is selected, enter a description for the cyber security approach. [Q:14.41-16195]

Incident Response (RBPS Metric 8.5.3)

The facility has a defined incident response system for cyber incidents: (Check one) [Q:14.41-16228]

- ○ 24x7x365 Computer emergency response function
- ○ Computer emergency response function
- ○ Other

If "Other" is selected, enter a description for the incident response system. [Q:14.41-16231]

Incident Reporting (RBPS Metric 8.5.4)

Does the facility have an incident reporting approach that ensures significant cyber events are reported to senior management and DHS US-CERT? [Q:14.41-16232]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the incident reporting approach. [Q:14.41-16234]

Post-Incident Measures (RBPS Metric 8.6)

The facility has the following post-incident measures: [Q:14.41-16242] **Indicate "Yes" for the post-incident measures that apply.**	**Yes**	**No**
Facility ensures that alternate site operations and recovery/reconstitution phases for the primary site include cyber security measures consistent with those in place for the original operational functions.	○	○
Facility has Continuity of Operations Plans.	○	○
Facility has IT Contingency Plans.	○	○
Facility has Disaster Recovery Plans.	○	○
Other	○	○

If "Other" is selected, enter a description for the post-incident measures. [Q:14.41-16243]

Network Operations and System Architecture (RBPS Metric 8.8.1-8.8.3, 8.7, General Data Collection - RBPS 8)

Documenting Business Needs (RBPS Metric 8.8.1)

Does the facility maintain the documentation of IT business needs? [Q:14.5-16295]

○ Yes

○ No

If "No" is selected, go to Network/System Architecture (RBPS Metric 8.8.3).

The facility documents a business need for all: [Q:14.51-16359] **Indicate "Yes" for the category that apply.**	**Yes**	**No**
Networks	○	○
Systems	○	○
Applications	○	○
Services	○	○

The facility documents a business need for all: [Q:14.51-16359] **Indicate "Yes" for the category that apply.**	**Yes**	**No**
Connections	○	○
Other	○	○

If "Other" is selected, enter a description for the specific category. [Q:14.51-16429]

Network/System Architecture (RBPS Metric 8.8.3)

Does the facility maintain the documented network/system architecture? [Q:14.5-16296]

○ Yes
○ No

If "No" is selected, go to Cyber Asset Identification (RBPS Metric 8.8.2).

The facility has established the following network housekeeping approach: [Q:14.51-16433] **Indicate "Yes" for the approach that apply.**	**Yes**	**No**
Facility identifies all network communication devices, media, and means and ensures they have appropriate cyber security controls in place.	○	○
Facility has a network diagram including nodes, interfaces, and information flows that reflects their current operating environment to ensure a comprehensive understanding of connectivity, dependency, and vulnerability.	○	○
Facility has an inventory of network nodes and interfaces that reflects their current operating environment.	○	○
Facility documents all systems, applications, and services running on their network and disables all unnecessary systems, applications, and services.	○	○
Other	○	○

If "Other" is selected, enter a description for the specific approach. [Q:14.51-16430]

Cyber Asset Identification (RBPS Metric 8.8.2)

Does the facility identify and evaluate its cyber assets? [Q:14.5-16307]

- ○ Yes
- ○ No

If "No" is selected, go to System Lifecycle (RBPS Metric 8.7).

The facility maintains the following preventive approach for its cyber assets: [Q:14.51-16434] **Indicate "Yes" for the approach that apply.**	**Yes**	**No**
Facility identifies critical information, assets, systems, and networks.	○	○
Facility identifies and evaluates potential vulnerabilities of the critical systems and networks	○	○
Facility disables all unnecessary system elements.	○	○
Facility implements appropriate security controls when vulnerabilities are detected.	○	○
Other	○	○

If "Other" is selected, enter a description for the specific approach. [Q:14.51-16432]

System Lifecycle (RBPS Metric 8.7)

Does the facility incorporate the cyber security in its system lifecycle? [Q:14.5-16330]

- ○ Yes
- ○ No

If "No" is selected, go to Backup Power for Cyber Systems (General Data Collection - RBPS 8).

Which approach the best describes the cyber security policy in the facility's system lifecycle? [Q:14.51-16658]

- ○ Facility integrates cyber security into the system lifecycle (design, procurement, installation, operation, and disposal).
- ○ Facility establishes security requirements for all systems and networks before they are put into operation, and for all operational systems and networks throughout their lifecycle.
- ○ Facility establishes security requirements for all critical systems and networks before they are put into operation, and for all critical operational systems and networks throughout their lifecycle.

○ Other

If "Other" is selected, enter a description for the specific approach. [Q:14.51-16659]

Backup Power for Cyber Systems (General Data Collection - RBPS 8)

Does the facility maintain the backup power equipment for the cyber system? [Q:14.5-16331]

○ Yes
○ No

If "No" is selected, go to Cyber Security Other (General Data Collection - RBPS 8).

The facility maintains the following backup power approach for the cyber system: [Q:14.51-16660] **Indicate "Yes" for the backup power approach that apply.**	**Yes**	**No**
Redundant offsite electrical power sources	○	○
Backup AC power system from onsite generators	○	○
Backup DC power system from UPS equipment	○	○
Other	○	○

If "Other" is selected, enter a description for the backup power system. [Q:14.51-16661]

Cyber Security Other (General Data Collection - RBPS 8)

Describe other cyber security measures in the details section. [Q:14.6-16662]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:14.88-15185]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:14.89-15186]

For more information, refer to the SSP instructions.

RBPS 9 – Response

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 9? [Q:15.0-18699]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 9.

RBPS 9 - Response

Does the facility have an emergency and security response organization and program to respond to site emergencies and security events? [Q:15.01-15515]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description: [Q:15.01-15516]

RBPS 9 - Response

Does the facility maintain a Crisis Management Plan for responding to an incident? [Q:15.015-15536]

- ○ Yes
- ○ No

If "No" is selected, go to Emergency Command Center (General Data Collection - RBPS 9).

RBPS 9 - Response

Select "Yes", if applicable: [Q:15.02-17474]

Indicate which of the following sections are included in the facility's Crisis Management Plan (provide answer for each - even if the answer is no or never):	**Yes**	**No**
Contingency plans.	○	○

Indicate which of the following sections are included in the facility's Crisis Management Plan (provide answer for each - even if the answer is no or never):	**Yes**	**No**
Continuity of operations plan.	○	○
Emergency response plans.	○	○
Emergency shutdown plans	○	○
Post-incident security plan (post-terrorist attack, security incident, natural disaster, etc.).	○	○
Evacuation plans.	○	○
Media response plans.	○	○
Notification control and contact requirements.	○	○
Re-entry/recovery plans.	○	○
Security response plans.	○	○
Documented agreements with off-site responder services, such as ambulance support, environmental restoration support, explosive device disposal support, fire fighting support, hazardous material spill/recovery support, marine support, and medical support.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.02-17476]

Responsibilities (RBPS Metric 9.1)

Does the Crisis Management Plan include the responsibility? [Q:15.03-15537]

Crisis Management Plan Responsibility	**Yes**	**No**
A crisis management team has been developed and is part of the emergency/security response organization.	○	○
Incident command is the primary responsibility of the emergency response organization.	○	○
On-scene command of an emergency or security event by local law enforcement is supported by the facility emergency/security response team.	○	○
Operational control of the facility and systems is the responsibility of the facility operators/supervisors as directed by the response team.	○	○

Crisis Management Plan Responsibility	Yes	No
Data capture and event/response time keeping is part of the responsibilities of the emergency/security response organization.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.03-15575]

Emergency Command Center (General Data Collection - RBPS 9)

Does the facility staff and operate an Emergency Operations Command Center?
[Q:15.04-15594]

○ Yes
○ No

Does the Emergency Operations Command Center have a backup power supply?
[Q:15.04-15621]

○ Yes
○ No

Does the facility staff and operate an Alternate Emergency Command Center? [Q:15.04-15622]

○ Yes
○ No

Does the Alternate Emergency Operations Command Center have a backup power supply?
[Q:15.04-15623]

○ Yes
○ No

Enter any additional relevant information: [Q:15.04-15624]

Security Command Center (General Data Collection - RBPS 9)

Does the facility staff and operate a Security Command and Control Center? [Q:15.04-15599]

- ○ Yes
- ○ No

Does the Security Command and Control Center have a backup power supply? [Q:15.04-15600]

- ○ Yes
- ○ No

Does the facility staff and operate an Alternate Security Command and Control Center? [Q:15.04-15601]

- ○ Yes
- ○ No

Does the Alternate Security Command and Control Center have a backup power supply? [Q:15.04-15602]

- ○ Yes
- ○ No

Enter any additional relevant information: [Q:15.04-15603]

Equipment (General Data Collection - RBPS 9)

Communications

What type of communication equipment does the facility maintain? [Q:15.06-15625]

Equipment - Communication	Yes	No
Bull horns	○	○
Computers	○	○
Personal Digital Assistants (PDA)	○	○
UHF radio	○	○
VHF radio	○	○

Equipment - Communication	Yes	No
Satellite telephone	○	○
Cellular telephone	○	○
Land-line telephone	○	○
Fax machine	○	○
Facility-wide alarm system	○	○
Redundant radio system that is interoperable with law enforcement and emergency response agencies	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.06-22791]

Response

What type of response equipment does the facility maintain? [Q:15.06-15626]

Equipment - Response	Yes	No
Camera / video recorder	○	○
Chemical spill containment kits and materials	○	○
Response support information package has been developed and available for responding LLEA	○	○
Current facility aerial photos and plot plans	○	○
Current facility drawings and system schematics	○	○
Firefighting equipment	○	○
HAZMAT - Hazardous Materials	○	○
Personal Protective Equipment (PPE)	○	○
SCBA - Self Contained Breathing Apparatus	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.06-22792]

Communication Radio System

Answer this question only if "Yes" was selected in question [Q:15.06-15626] for the item "Redundant radio system that is interoperable with law enforcement and emergency response agencies"

What type of redundant radio system is employed? [Q:15.07-15640]

Responder Information (RBPS Metric 9.1)

Have response/support agreement been developed with local law enforcement agencies? [Q:15.1-15853]

- ○ Yes
- ○ No

Internal Emergency Responders

Internal Emergency Responder	What best describes the responder? [Q:15.1-15642] (Choose one: Available not dedicated, Available and dedicated, Not Available)	What is the response time (minutes)? [Q:15.11-15858]
First responders - Emergency Medical Technician (EMT)		
First responders - Fire suppression		
First responders - Spill containment		
Other		

If "Other" is selected, enter a description: [Q:15.1-22850]

External Emergency Responders

External Emergency Responder	What best describes the responder? [Q:15.1-15644] (Choose one: Available not dedicated, Available and dedicated, Not Available)	What is the response time (minutes)? [Q:15.11-15877]
Ambulance support		
Environmental restoration support		
Explosive device disposal support		
Firefighting support		
Hazardous material recovery support		
Marine support		
Medical support		
SWAT		
Other		

If "Other" is selected, enter a description: [Q:15.1-22851]

Drills/Exercises (RBPS Metric 9.3 and 9.4)

How often does the site conduct response drills and exercises? [Q:15.12-15885]

(Choose one: monthly, quarterly, semi-annually, annually, biennially, triennially, never)

How often are other drills and exercises conducted? [Q:15.12-15886]

(Choose one: monthly, quarterly, semi-annually, annually, biennially, triennially, never)

If other drills and exercises are conducted, enter a description. [Q:15.12-15887]

Process Safeguards (RBPS Metric 9.3)

Is the Process Safeguard applicable? [Q:15.13-15890]

Process Safeguards	Yes	No
Facility has an automated control system for process units containing COI that are capable of rapidly putting the COI in a safe and stable condition.	○	○
Facility has procedures in place to use these automated control systems in case of an emergency.	○	○
Process safeguards have a backup power supply.	○	○
Other	○	○

What percentage of automated control systems containing COI are capable of rapidly putting the COI in a safe and stable condition? [Q:15.13-15982]

If "Other" is selected, enter a description: [Q:15.13-15897]

Outreach (RBPS Metric 9.4)

Select "Yes" if the outreach is applicable to the facility: [Q:15.14-15891]

Outreach	Yes	No
Facility has an active outreach program to the community and local law enforcement	○	○
Facility participates in a Local Emergency Planning Committee (LEPC)	○	○
Facility participates in a Community Hazards Emergency Response-Capability Assurance Process (CHER-CAP)	○	○
Facility participates in Buffer Zone Protection Program (BZPP) activities	○	○
Facility participates in a Neighborhood Watch Program	○	○
Facility participates in security-related drills and exercises in conjunction with off-site responder organizations	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.14-15896]

Emergency Power (RBPS Metric 9.2)

Does the facility have emergency backup power for all communications, emergency notification, security systems, and process control systems? [Q:15.15-15892]

○ Yes

○ No

Do the emergency redundant backup power systems have a redundant back up system? [Q:15.15-15893]

- ○ Yes
- ○ No
- ○ Not applicable

Communications (RBPS Metric 9.2)

Select "Yes" if the communication system is applicable to the facility: [Q:15.16-15894]

Communications	Yes	No
The facility utilizes various communications systems and methods to provide emergency and security notifications and communications both internal and external to the facility	○	○
Local law enforcement agencies are informed in a timely manner of changes in facility layout/operations that may affect their response	○	○
Local law enforcement agency personnel have been invited to facility orientation tours, meetings, presentations, etc.	○	○
The site has a timely communication with DHS subsequent to a loss of regulated materials	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:15.16-15895]

Community-wide Communications (RBPS Metric 9.2)

Community-wide Communication	Select "Yes" if the community-wide communication is applicable to the facility: [Q:15.16-15945]		Is there a backup power supply available with the communication? [Q:15.16-15947]	
	Yes	No	Yes	No
Telephone call trees	○	○	○	○
Automatic dialer/messaging	○	○	○	○
Community siren(s)	○	○	○	○

Community-wide Communication	Select "Yes" if the community-wide communication is applicable to the facility: [Q:15.16-15945]		Is there a backup power supply available with the communication? [Q:15.16-15947]	
Wide area address system	○	○	○	○
Local radio/television	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:15.16-15946]

Facility-wide Communications (RBPS Metric 9.2)

Facility-wide Communication	Select "Yes" if the facility-wide communication is applicable to the facility: [Q:15.16-15948]		Is there a backup power supply available with the communication? [Q:15.16-15949]	
	Yes	**No**	**Yes**	**No**
Plant telephone system	○	○	○	○
Local plant siren	○	○	○	○
Plant PA system	○	○	○	○
Fire/PA combination system	○	○	○	○
Pagers	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:15.16-15950]

Facility Communications (RBPS Metric 9.2)

Facility Communication	Select "Yes" if the facility communication is applicable to the facility: [Q:15.16-15951]		Is there a backup power supply available with the communication? [Q:15.16-15952]	
	Yes	No	Yes	No
Direct wire / LAN / cable / Internet	○	○	○	○
Integrated electronic telecommunications with responders	○	○	○	○
Radio/radio-telephone to communicate	○	○	○	○
VHF/marine radio	○	○	○	○
UHF radio	○	○	○	○
Satellite communications	○	○	○	○
Plant telephone / cell phone / PDA	○	○	○	○
Pagers	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:15.16-15953]

Security Communications (RBPS Metric 9.2)

Security Communication	Select "Yes" if the security communication is applicable to the facility: [Q:15.16-15954]		Is there a backup power supply available with the communication? [Q:15.16-15955]	
	Yes	No	Yes	No
Direct wire / LAN / cable / Internet	○	○	○	○
Integrated electronic telecommunications with responders	○	○	○	○
Radio/radio-telephone to communicate	○	○	○	○

Security Communication	Select "Yes" if the security communication is applicable to the facility: [Q:15.16-15954]		Is there a backup power supply available with the communication? [Q:15.16-15955]	
VHF/marine radio	○	○	○	○
UHF radio	○	○	○	○
Satellite communications	○	○	○	○
Plant telephone / cell phone / PDA	○	○	○	○
Pagers	○	○	○	○
Other	○	○	○	○

If "Other" is selected, enter a description: [Q:15.16-15956]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:15.88-15200]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:15.89-15205]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 10 – Monitoring

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 10? [Q:16.0-18700]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 10.

System Inspection and Testing (General Data Collection - RBPS 10, RBPS Metric 10.1, 10.3)

Does the facility maintain written procedures to mitigate a failure of the security systems? [Q:16.005-15260]

- ○ Yes
- ○ No

Does the facility conduct an inspection of restricted areas, access doors and gates, vehicle barriers, lighting, or any security related equipment? [Q:16.005-15261]

- ○ Yes
- ○ No

Does the facility perform a testing and maintenance of the security system? [Q:16.005-15262]

- ○ Yes
- ○ No

If "Yes" is selected for [Q:16.005-15260], answer Monitoring (RBPS Metric 10.3 and General Data Collection - RBPS 10).
If "Yes" is selected for [Q:16.005-15261], answer Inspection (RBPS Metric 10.1).
If "Yes" is selected for [Q:16.005-15262], answer Testing (RBPS Metric 10.1)and Maintenance (RBPS Metric 10.3).
If "No" is selected for answered to all three above questions, skip Records (RBPS Metric 10.4).

Monitoring (RBPS Metric 10.3 and General Data Collection - RBPS 10)

The facility maintains the following written procedures to prevent a failure of the security systems (provide answer for each - even if the answer is no or never): [Q:16.01-15263] **Indicate "Yes", if applicable**	**Yes**	**No**
Facility has a written plan to regularly inspect, test, calibrate, repair and maintain security systems and systems related to security.	○	○

The facility maintains the following written procedures to prevent a failure of the security systems (provide answer for each - even if the answer is no or never): [Q:16.01-15263] **Indicate "Yes", if applicable**	**Yes**	**No**
Facility has a written procedure to record and repair failures, deficiencies, and malfunctions of security and security-related equipment.	○	○
Facility has designated an individual or individuals in writing whose responsibility it is to inspect, test, maintain and calibrate security related equipment. This individual is responsible for investigating and resolving all malfunctions and recommending repairs or modifications of this equipment.	○	○
Other	○	○

If "Other" is selected, enter a description for the procedures. [Q:16.01-15266]

Inspection (RBPS Metric 10.1)

The facility conducts the following inspections (provide answer for each - even if the answer is no or never): [Q:16.02-15268]	**Indicate frequency, if applicable** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Perimeter and restricted area barriers are inspected to ensure their integrity on a periodic basis.	
The clearance between the bottom of the fence and the ground is inspected to ensure that the gap does not permit access under the barrier, due to settling, washout, etc.	
Doors and gates are inspected and tested for proper operations on a periodic basis.	
The locking mechanisms and/or access control devices (such as keypads) on doors and gates are inspected and tested to ensure that they are operating properly to secure the door/gate.	
Vehicle barriers are inspected for miss-alignment, degradation, and proper operation.	
Facility inspects all CCTV cameras to ensure functionality.	
Facility inspects lighting systems to ensure functionality.	
Facility tests all alarms to ensure functionality.	

The facility conducts the following inspections (provide answer for each - even if the answer is no or never): [Q:16.02-15268]	**Indicate frequency, if applicable** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Facility tests its emergency notification equipment.	
Facility tests its communications systems.	
Other	

If "Other" is selected, enter a description for the specific inspection. [Q:16.02-15267]

Testing (RBPS Metric 10.1)

The facility performs the following forms of testing (provide answer for each - even if the answer is no or never): [Q:16.03-15269] **Indicate "Yes", if applicable**	**Yes**	**No**
Periodic test of security systems and equipment are conducted to demonstrate the correct operation of all equipment, procedures, processes and systems that support the security infrastructure.	○	○
Testing validates that the equipment and systems conform to original specifications and operate in the required environments and that supporting procedures and processes remain valid and workable.	○	○
The site uses dynamic tests to verify that security assets function independently or in consort with each other (as required), to satisfy operational requirements.	○	○
CCTV camera and recording components are tested periodically to ensure operability.	○	○
The site uses functional tests to verify that security procedures work.	○	○
Devices/systems found to be inoperative or not operating properly are reported and repaired promptly.	○	○
The site uses static tests to determine if the essential components of the security assets (personnel, equipment, system, etc.) meet the specification and design requirements of the organization.	○	○

The facility performs the following forms of testing (provide answer for each - even if the answer is no or never): [Q:16.03-15269] **Indicate "Yes", if applicable**	**Yes**	**No**
Testing validates that any sources of back-up power are adequate and operational.	○	○
Other	○	○

If "Other" is selected, enter a description for the specific test procedure. [Q:16.03-15270]

Maintenance (RBPS Metric 10.3)

The facility performs the following maintenance process of the security system (provide answer for each - even if the answer is no or never): [Q:16.03-15271] **Indicate "Yes", if applicable**	**Yes**	**No**
Deficiencies with perimeter and restricted area barriers, doors and gates are reported and promptly corrected.	○	○
Security equipment such as gates, cameras, lights, alarms, keypad entry systems are tested, calibrated and maintained according to the manufacturers' recommendations.	○	○
Other	○	○

If "Other" is selected, enter a description for the maintenance process. [Q:16.03-15272]

Records (RBPS Metric 10.4)

The facility documents and maintains the following records (provide answer for each - even if the answer is no or never): [Q:16.04-15273] **Indicate "Yes", if applicable**	**Yes**	**No**
Records of inspections performed on security equipment/systems are maintained by the facility.	○	○
Records of tests performed on security equipment/systems are maintained by the facility.	○	○

The facility documents and maintains the following records (provide answer for each - even if the answer is no or never): [Q:16.04-15273] **Indicate "Yes", if applicable**	**Yes**	**No**
Records of maintenance performed on security equipment/systems are maintained by the facility.	○	○
Records of improvements to security equipment/systems are maintained by the facility.	○	○
Records of repairs to security equipment/systems are maintained by the facility.	○	○
Facility documents and maintains records of all security and security-related equipment inspections, testing, and preventative maintenance conducted by non-resident contractor.	○	○
Other	○	○

If "Other" is selected, enter a description for the records maintenance. [Q:16.04-15274]

System Repairs and Compensatory Measures (RBPS Metric 10.2)

Does the facility implement temporary/compensatory measures in the event of security systems deficiencies of operation? [Q:16.2-15275]

○ Yes
○ No

Reporting Non-Routine Incidents (General Data Collection - RBPS 10)

Does the facility properly document and promptly report non-routine outages, equipment failures, and malfunctions, to the SSO? [Q:16.2-17307]

○ Yes
○ No
○ Other

If "Other" is selected, enter a description for the non-routine incident reporting. [Q:16.2-15291]

Temporary/Compensatory Measures (RBPS Metric 10.2)

If "No" is selected for Does the facility implement temporary/compensatory measures in the event of security systems deficiencies of operation? [Q:16.2-15275], go to Planned Measures.

In the event of security system deficiencies of operation, appropriate temporary/compensatory measures are implemented (provide answer for each - even if the answer is no or never): [Q:16.21-15277] **Indicate "Yes", if applicable**	**Yes**	**No**
Remote surveillance via CCTV is used to provide surveillance over affected sensors/areas.	○	○
Deployment of back-up hardware to replace degraded hardware.	○	○
Security patrols within and outside the perimeter conducted to compensate for the loss of security system(s).	○	○
Security/facility personnel can be posted to provide equivalent levels of protection.	○	○
Operations personnel are used to provide surveillance of areas to identify unauthorized activities and/or access to materials.	○	○
Facility is able to implement appropriate temporary security measures in response to non-routine outages, equipment failures, and malfunctions.	○	○
Other	○	○

If "Other" is selected, enter a description for the temporary/compensatory measures. [Q:16.21-15278]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:16.88-15222]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:16.89-15230]

For more information, refer to the SSP instructions.

RBPS 11 – Training

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 11? [Q:17.0-18701]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 11.

Training Policy/Procedures (RBPS Metric 11.1)

Has the facility developed and implemented a security awareness and training program (SATP) to satisfy all training requirements? [Q:17.003-15296]

- ○ Yes
- ○ No

If "No" is selected, go to Training Records (General Data Collection - RBPS 11).

Training Policy/Procedures (RBPS Metric 11.1)

Indicate if the SATP contains the following information (check all that apply): [Q:17.0005-15297]

For each checked response, answer the questions that are relevant. Once completed, go to Training Records (General Data Collection - RBPS 11).

☐	Training	*Site Security Officer Training (RBPS Metric 11.1)* *Security Personnel Training (RBPS Metric 11.1)* *All Employees Training (RBPS Metric 11.2)* *Training Methods (RBPS Metrics 11.1 and 11.2)*
☐	Exercises	*Training Exercise (RBPS Metric 11.3)*
☐	Drills	*Training Drills (RBPS Metric 11.3)*
☐	Tests	*Training - Testing of Security Equipment (General Data Collection - RBPS 11)*
☐	Joint Initiatives	*Joint Initiatives (RBPS Metric 11.3)*
☐	Other	

If "Other" is selected, please describe. [Q:17.005-15298]

Site Security Officer Training (RBPS Metric 11.1)

Please select training frequency for the Site Security Officer (SSO)/Assistant SSO on the following (provide answer for each - even if the answer is never): [Q:17.01-15592]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Security Laws and Regulation	
Threats	
Security Organization/Duties and Responsibilities	
CSAT - Top Screen	
CSAT - Security Vulnerability Assessment (SVA)	
CSAT - Site Security Plan (SSP)	
CSAT - Personnel Screening Database	
Security Measures and Management of SSPs	
Requirements of SSP	
Drills and Training	
Inspection and Screening	
Recordkeeping	
Other	

If "Other" is selected, please describe. [Q:17.01-15646]

Security Personnel Training (RBPS Metric 11.1)

Please select training frequency for the SSO/Assistant SSO and Security Personnel on the following (provide answer for each - even if the answer is never): [Q:17.02-15647]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Knowledge of current security threats and patterns	
Crowd management and control techniques	
Security related communications	
Knowledge of emergency procedures, crisis management plan, and contingency plans	
CVI Training	
Operation of security equipment and systems	
Testing, calibration, and maintenance of security equipment and systems	
Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores	
Other	

If "Other" is selected, please describe. [Q:17.02-15648]

All Employees Training (RBPS Metric 11.2)

Please select training frequency for the SSO/Assistant SSO and Security Personnel and all employees on the following (provide answer for each - even if the answer is never): [Q:17.03-15649]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Recognition and detection of explosive materials	
Recognition and detection of explosive devices	
Recognition and detection of Improvised materials	
Recognition and detection of Vehicle Borne Improvised Explosive Devices (VBIEDs)	

Security Personnel Training (RBPS Metric 11.1)

Please select training frequency for the SSO/Assistant SSO and Security Personnel on the following (provide answer for each - even if the answer is never): [Q:17.02-15647]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Knowledge of current security threats and patterns	
Crowd management and control techniques	
Security related communications	
Knowledge of emergency procedures, crisis management plan, and contingency plans	
CVI Training	
Operation of security equipment and systems	
Testing, calibration, and maintenance of security equipment and systems	
Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores	
Other	

If "Other" is selected, please describe. [Q:17.02-15648]

All Employees Training (RBPS Metric 11.2)

Please select training frequency for the SSO/Assistant SSO and Security Personnel and all employees on the following (provide answer for each - even if the answer is never): [Q:17.03-15649]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Recognition and detection of explosive materials	
Recognition and detection of explosive devices	
Recognition and detection of Improvised materials	
Recognition and detection of Vehicle Borne Improvised Explosive Devices (VBIEDs)	

Please select training frequency for the SSO/Assistant SSO and Security Personnel and all employees on the following (provide answer for each - even if the answer is never): [Q:17.03-15649]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Recognition and detection of Hand-carried weapons	
Recognition and detection of Surveillance devices (e.g., camera phones)	
Recognition of characteristics and behavioral patterns of persons who are likely to threaten security	
General Techniques used to circumvent security measures	
Relevant provisions of the Site Security Plan (SSP)	
The meaning and the consequential requirements of the different DHS Threat Levels as they apply to them, including emergency procedures and contingency plans	
Recognition of a Security Incident	
Reporting of a Security Incident	
Emergency Procedures	
Operating Security Equipment	
Operation of security equipment and systems	
Other	

If "Other" is selected, please describe. [Q:17.03-15650]

Training Methods (RBPS Metrics 11.1 and 11.2)

Please select methods employed in training the SSO/Assistant SSO (check all that apply): [Q:17.04-15651]

- ☐ Hands-on activities
- ☐ Hand-outs, bulletin boards, etc
- ☐ Lectures
- ☐ On-line or interactive programs
- ☐ Orientations
- ☐ Seminars

- ☐ Workshops
- ☐ Briefings
- ☐ Video
- ☐ Other

If "Other" is selected, please describe. [Q:17.04-15652]

Please select methods employed in training Security Personnel (check all that apply): [Q:17.04-18868]

- ☐ Hands-on activities
- ☐ Hand-outs, bulletin boards, etc
- ☐ Lectures
- ☐ On-line or interactive programs
- ☐ Orientations
- ☐ Seminars
- ☐ Workshops
- ☐ Briefings
- ☐ Video
- ☐ Other

If "Other" is selected, please describe. [Q:17.04-18869]

Please select methods employed in training other employees (check all that apply): [Q:17.04-18870]

- ☐ Hands-on activities
- ☐ Hand-outs, bulletin boards, etc
- ☐ Lectures
- ☐ On-line or interactive programs
- ☐ Orientations
- ☐ Seminars
- ☐ Workshops
- ☐ Briefings
- ☐ Video
- ☐ Other

If "Other" is selected, please describe. [Q:17.04-18871]

Training Exercise (RBPS Metric 11.3)

Does the facility conduct security exercises? [Q:17.05-15653]

- ○ Yes
- ○ No

If "No" is selected, go back to Training Policy/Procedures (RBPS Metric 11.1).

Indicate if the security exercises include the following (provide answer for each - even if the answer is no or never): [Q:17.055-15654] **Select "Yes", if applicable**	**Yes**	**No**
Facility conducts exercises to provide simulations that promote preparedness, improve the response capability, validate plans, policies, procedures and systems, and determine the effectiveness of the command, control, and communication functions and event-scene activities.	○	○
Facility conducts exercises as realistic rehearsals or simulations of security related events, in which individuals and security measures demonstrate the tasks expected of them in a real incident.	○	○
Facility evaluates exercises to identify systemic weaknesses and suggest corrective actions to enhance security.	○	○
Facility evaluates exercises to validate elements, both individually and collectively, of the organization's security measures.	○	○
Following an exercise, the site completes a comprehensive debriefing and after-action report.	○	○
The facility incorporates lessons learned and recommendations into corrective action plans and feedback to improve the training program.	○	○
Other	○	○

If "Other" is selected, please describe. [Q:17.055-15655]

Frequency of Tabletop Exercises [Q:17.055-15726]
Tabletop exercises simulate security incidents in an informal, stress-free environment to elicit constructive discussion as participants examine and resolve problems based on existing plans, policies and procedures. There is minimal attempt at simulation, no utilization of equipment or deployment of resources, and no time pressures.

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triiennially
- ○ never

Frequency of Functional Exercises [Q:17.055-15921]
Functional exercises fully simulated and interactive exercises. They validate the capability of a group (i.e., protective force) or facility to respond to a simulated event testing one or more procedures and/or function of the facility's security plan. Functional exercises focus on policies, procedures, roles and responsibilities of single or multiple security functions before, during, or after a security related event.

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triiennially
- ○ never

Frequency of Full-Scale Exercises [Q:17.055-15923]
Full-scale exercises simulate actual emergency conditions and are field exercises designed to evaluate the operational capabilities of the organization's security posture and response capability in a highly stressful environment.

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triiennially
- ○ never

Training Drills (RBPS Metric 11.3)

Does the facility conduct drills? [Q:17.06-15727]

- ○ Yes
- ○ No

If "No" is selected, go back to Training Policy/Procedures (RBPS Metric 11.1).

Indicate if the drills include the following (provide answer for each - even if the answer is no or never): [Q:17.065-15728] **Select "Yes", if applicable**	**Yes**	**No**
Facility conducts drills as coordinated, supervised activities normally used to exercise a single specific operation or function.	○	○
Facility conducts drills to provide training with new equipment, to develop new policies or procedures, or to practice and maintain current skills.	○	○
Facility conducts drills to validate the capability of an organization to respond to a simulated incident.	○	○

Indicate if the drills include the following (provide answer for each - even if the answer is no or never): [Q:17.065-15728] **Select "Yes", if applicable**	**Yes**	**No**
Facility compiles lessons learned and recommendations for each drill activity.	○	○
The facility incorporates lessons learned and recommendations into the drilling procedure to improve the training program.	○	○
Other	○	○

If "Other" is selected, please describe. [Q:17.065-15729]

Please select the frequency of the drills [Q:17.065-15730]

○ monthly ○ quarterly ○ semi-annually
○ annually ○ biennially ○ triennially
○ never

Please list the equipment or topic of the conducted drills [Q:17.065-15731]

Training - Testing of Security Equipment (General Data Collection - RBPS 11)

Does the facility conduct testing of security equipment? [Q:17.07-15732]

○ Yes
○ No

If "No" is selected, go back to Training Policy/Procedures (RBPS Metric 11.1).

Indicate the frequency of the following types of testing (provide answer for each - even if the answer is no or never): [Q:17.075-15733]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Static testing frequency to compare the security equipment against required specifications	

Indicate the frequency of the following types of testing (provide answer for each - even if the answer is no or never): [Q:17.075-15733]	**Please select the training frequency** (Choose one: monthly, quarterly, semi-annually, annually, biennually, triennially, never)
Dynamic testing frequency to determine whether individual pieces of security equipment work well together (i.e., lighting and CCTV)	
Functional testing frequency to verify that procedures for operating the security equipment and systems in the backup environment are correct	
Other	

If "Other" is selected, please describe. [Q:17.075-15899]

Indicate who conducts the testing of security equipment (provide answer for each - even if the answer is no or never): [Q:17.075-15735] **Select "Yes", if applicable**	**Yes**	**No**
Facility uses resident contractors to conduct testing of security equipment.	○	○
Facility uses non-resident contractors to conduct testing of security equipment.	○	○
Facility uses employees to conduct testing of security equipment.	○	○
Other	○	○

If "Other" is selected, please describe. [Q:17.075-15734]

Joint Initiatives (RBPS Metric 11.3)

Does the facility participate in joint initiatives with other organizations/agency (i.e., facility and local law enforcement) exercises to rehearse coordinated security related procedures? [Q:17.08-15741]

○ Yes

○ No

If "Yes" is selected for the above question, please indicate the frequency of joint exercises [Q:17.08-15742]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

Training Records (General Data Collection - RBPS 11)

Does the facility maintain employee training records? [Q:17.09-15746]

- ○ Yes
- ○ No

If "No" is selected, go to Planned Measures.

Indicate the type of employees for whom the training records are maintained (check all that apply): [Q:17.1-15748]

- ☐ All employees
- ☐ Regular contractor employees
- ☐ Visitors
- ☐ Temporary contractor employees
- ☐ Other

If "Other" is selected, please describe. [Q:17.1-15765]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:17.88-15223]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:17.89-15231]

For more information, refer to the SSP instructions.

RBPS 12 – Personnel Surety

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 12? [Q:18.0-18702]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 12.

Policy (RBPS Metric 12.1 and 12.2)

Select "Yes" for all procedures that the facility implements for personnel surety.

Procedure [Q:18.1-16688]	**Yes**	**No**
Facility has an existing program for conducting background investigations on its employees with unescorted access to critical or restricted areas.	○	○
Facility denies access to critical or restricted areas until successful background investigation for existing employee is completed.	○	○
Contractors certify that they have an employee background screening program and that the employees working at the facility have successfully passed the screening process.	○	○
Facility does not have a program for conducting background investigations on its employees.	○	○
Other	○	○

If "Other" is selected, enter a description of the procedures in use: [Q:18.1-16689]

After receiving preliminary approval of the Site Security Plan (SSP), will the facility perform background investigations on existing employees with unescorted access to critical or restricted areas and will the facility deny access to these critical or restricted areas until successful background investigations for existing employees are completed? [Q:18.1-16878]

- ○ Yes
- ○ No

After receiving preliminary approval of the Site Security Plan (SSP), the facility will perform background investigations on existing employees with unescorted access to critical or restricted areas within (months):
[Q:18.1-16880]

Background Investigations (RBPS Metric 12.3)

Select "Yes" for all background investigation measures that are employed by the facility.

Background Investigation Measure [Q:18.2-16817]	**Yes**	**No**
Applicants and individuals requiring unescorted access to the facility are required to present Form I-9 identification document to establish their identity and/or employment eligibility.	○	○
Applicants and individuals requiring unescorted access to the facility complete criminal history and financial information release forms to be used as part of the background investigation to establish if any disqualifying criminal history exists.	○	○
Applicant and individuals requiring unescorted access to the facility identities are cross-checked against DHS approved Terrorist Screening Database to establish the existence of any terrorist organizations/support organization ties before unescorted access is granted.	○	○
Other	○	○

If "Other" is selected, enter a description for the background investigation: [Q:18.2-16943]

Terrorist Screening Database Records (RBPS Metric 12.4)

Upon notification from DHS, that DHS has implemented the capability to perform TSDB background checks on behalf of high-risk chemical facilities to identify individuals with terrorist ties, will the facility implement a process to submit to DHS personally identifiable information (See. Vol. 72 FR 17709) about facility personnel, and as appropriate unescorted visitors, with access to the restricted areas or critical assets necessary to perform the background check against the TSDB?
[Q:18.3-16663]

○ Yes

○ No

If "Yes" is selected, skip question [Q:18.39-18800].
If "No" is selected, answer question [Q:18.39-18800] and go to Background Investigation Frequency (RBPS Metric 12.2).

How will the facility identify facility personnel, and as appropriate unescorted visitors, with access to the restricted areas or critical assets with terrorist ties?
[Q:18.39-18800]

Will the facility process for submitting personally identifiable information to DHS:

a) Describe when the facility will initially provide information about any individuals who have access to a restricted area or a critical asset?
[Q:18.31-18801]

- ○ Yes
- ○ No

b) Describe when updates and corrections to erroneous information previously submitted to DHS will occur after they are discovered?
[Q:18.31-18802]

- ○ Yes
- ○ No

c) Describe when the facility will notify DHS after an individual no longer has access to restricted areas or critical assets at the facility?
[Q:18.31-18803]

- ○ Yes
- ○ No

Terrorist Screening Database Records (RBPS Metric 12.4)

Will the facility provide notification to facility personnel, and as appropriate unescorted visitors, with access to the restricted areas or critical assets that personal information about them has been or will be submitted to DHS to determine if they have terrorist ties?
[Q:18.32-18804]

- ○ Yes
- ○ No

Select "Yes" for all categories of people that are screened.

Persons Screened [Q:18.38-16665]	**Yes**	**No**
Employees who have unescorted access to critical or restricted areas	○	○

Persons Screened [Q:18.38-16665]	**Yes**	**No**
Contractors who have unescorted access to critical or restricted areas	○	○
All security staff including contractors	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:18.38-16686]

Does the facility maintain a list of facility personnel, and as appropriate unescorted visitors, with access to the restricted areas or critical assets?
[Q:18.38-16664]

○ Yes
○ No

Background Investigation Frequency (RBPS Metric 12.2)

Does the facility identify grounds for denying access or employment to individuals subject to a background check?
[Q:18.4-16838]

○ Yes
○ No

Does the facility repeat background investigations on existing employees at regular intervals?
[Q:18.4-16837]

○ Yes
○ No

If "No" is selected, go to Access Control (General Data Collection - RBPS 12)

What is the interval for repeating background investigations? [Q:18.42-16863]

○ Every year
○ Every 2 years
○ Every 3 years
○ Every 4 years
○ Every 5 years
○ Every 6 years
○ Every 7 years
○ Other

If "Other" is selected, enter a description of the background investigation frequency:
[Q:18.42-22795]

Access Control (General Data Collection - RBPS 12)

Select "Yes" for all access control measures that are implemented by the facility.

Access Control Measure [Q:18.5-16871]	**Yes**	**No**
All individuals having unescorted access to secure areas have successfully completed a background investigation.	○	○
Individuals allowed unescorted access to a restricted/secure area have successfully completed a background investigation.	○	○
Individuals with access to security sensitive information have successfully completed a background investigation.	○	○
Individuals engaged in security activities have successfully completed a background investigation.	○	○
Individuals granted unescorted access to the facility are required to attend security awareness training at the facility.	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:18.5-16944]

Audit (RBPS Metric 12.4)

Does the facility have a background check program?
[Q:18.6-16435]

○ Yes

○ No

If "No" is selected, go to Planned Measures.

Does the facility audit its background check program?
[Q:18.7-16436]

- ○ Yes
- ○ No

If "No" is selected, go to Planned Measures

What percentage of background checks are audited?
[Q:18.72-16437]

- ○ Less than 5%
- ○ 5% - 9%
- ○ 10% - 14%
- ○ 15% - 24%
- ○ 25% - 49%
- ○ 50% or more

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:18.88-15224]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:18.89-15232]

For more information, refer to the SSP instructions.

RBPS 13 – Elevated Threats

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 13?
[Q:19.0-18703]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 13.

Policy (General Data Collection - RBPS 13)

Does the facility have a documented process for increasing security measures during periods of elevated threats tied to the National Terrorism Advisory System (NTAS)?
[Q:19.1-16350]

- ○ Yes
- ○ No

Security Measures (RBPS Metric 13.1)

What level of security measures are implemented during periods of elevated threat as designated under NTAS?
[Q:19.1-16364]

- ○ Commensurate to the designated threat level.
- ○ Greater than the designated threat level.
- ○ Less than the designated threat level.
- ○ No additional security measure implemented.
- ○ Other

If "Other" is selected, enter a description. [Q:19.1-16358]

Security Measures (RBPS Metric 13.1)

Select "Yes" for all the measures that the facility uses when an Elevated Threat Alert is issued that applies to the facility.

Elevated Threat Level Security Measures [Q:19.2-16736]	**Yes**	**No**
Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations	○	○
Taking additional precautions at public events held on-site and possibly considering alternative venues or even cancellation	○	○
Preparing to execute contingency procedures, such as moving to an alternate facility or dispersing their workforce	○	○
Restricting threatened facility access to essential personnel only	○	○
Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources	○	○
Additional barriers at vehicle access points and around critical process units to control traffic and increase standoff distances	○	○
Additional illumination for remote areas	○	○
Decrease the number of personnel authorized to be on-site	○	○
Extend physical protection of vulnerable points, including off-site critical facilities	○	○
Increased frequency of perimeter patrols	○	○
Increased security force allocations	○	○
Increased railcar inspections	○	○
Increased personnel and vehicle screening inspections	○	○
Mandatory visitor escorts	○	○
Minimize the number of gates in use	○	○
Off-site mail handling	○	○
Parking restrictions	○	○
Postpone projects and activities where high risk chemicals are more exposed or vulnerable	○	○
Real-time reporting capability between the security control center and the main process control center	○	○
Reinforced barriers at remote or unused gates	○	○

Elevated Threat Level Security Measures [Q:19.2-16736]	**Yes**	**No**
Other	○	○

If "Other" is selected, enter a description. [Q:19.2-16737]

Security Measures (RBPS Metric 13.1)

Select "Yes" for all the measures that the facility uses when an Imminent Threat Alert is issued that applies to the facility.

Imminent Threat Level Security Measures [Q:19.3-16726]	**Yes**	**No**
Increasing or redirecting personnel to address critical emergency needs	○	○
Decrease the number of personnel on-site to "essential" personnel only	○	○
Night vision devices for security force	○	○
Constant perimeter patrols	○	○
Maximum security force staffing	○	○
100% railcar inspections	○	○
100% personnel and vehicle screening inspections	○	○
No visitors allowed on-site	○	○
No parking on-site (except vehicles always kept inside the restricted area)	○	○
Lock down the control center to deny access to unauthorized personnel	○	○
May have arrangements in place to secure armed response capability utilizing any combination of proprietary, contract, local, state and/or federal resources where safety at the facility is not compromised	○	○
Other	○	○

If "Other" is selected, enter a description. [Q:19.3-16727]

Response Time (RBPS Metric 13.2)

Indicate the time period in which the facility has the capability to implement increased levels of security in response to DHS elevating the NTAS threat level, while maintaining the measures already in use during normal operating periods.
[Q:19.3-16732]

- ○ Up to 8 hours
- ○ From 8 to 12 hours
- ○ From 12 to 24 hours
- ○ More than 24 hours

Other Measures (General Data Collection - RBPS 13)

Describe other elevated threat response elements in use at the facility.
[Q:19.3-16914]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:19.88-15225]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:19.89-15233]

For more information, refer to the SSP instructions.

RBPS 14 – Specific Threats

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 14? [Q:20.0-18704]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 14.

Policy (RBPS Metric 14.1 and 14.2)

Does the facility's threat policy include this feature? Select "Yes" for all that apply.

Threat Policy [Q:20.01-16186]	**Yes**	**No**
The facility has the ability to identify and implement measures if the Assistant Secretary communicates facility specific threats, vulnerabilities or risks.	○	○
Measures identified and implemented to address facility specific threats, vulnerabilities or risks meet the metrics for all other applicable RBPS for the facility.	○	○
Measures identified and implemented to address facility specific threats, vulnerabilities or risks are documented in the SSP.	○	○
Measures for responding to specific threats include idling the facility.	○	○
Measures for responding to specific threats include safe shutdown of the facility.	○	○
The facility has a documented Chain of Command approval process for rapid identification and implementation of measures in response to specific threats.	○	○
Other	○	○

If "Other" is selected, enter a description for the threat policy. [Q:20.01-17202]

Training (RBPS Metric 14.3)

Have all relevant employees been trained on the potential measures implemented to address facility specific threats, vulnerabilities, or risks?
[Q:20.02-16188]

- ○ Yes
- ○ No

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:20.88-15226]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:20.89-15234]

For more information, refer to the SSP instructions.

RBPS 15 – Reporting Significant Security Incidents

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 15? [Q:21.0-18705]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 15.

Policy (RBPS Metrics 15.1 and 15.2)

What procedures does the facility employ for security incidents?

Policy [Q:21.05-16940]	**Yes**	**No**
Facility has written procedures to identify the types of security incidents to report to facility security personnel.	○	○
Facility has written procedures to identify the significant security incidents to report to facility personnel, local law enforcement and DHS.	○	○
Facility has written procedures on identifying and reporting near miss security incidents.	○	○
Facility has written procedures identifying facility personnel that are responsible for reporting these security incidents.	○	○
Facility has written procedures on to whom to report security incidents.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:21.05-17004]

Reporting Procedures (RBPS Metric 15.1)

Does the facility have documented procedures (or facility alarm) for detection of suspicious person, vehicle, or device and appropriate reporting requirements to facility security personnel and, if appropriate, local law enforcement or DHS? [Q:21.1-16941]

- ○ Yes
- ○ No

What security incidents has the facility identified as significant?

Security Procedures [Q:21.1-16942]	**Yes**	**No**
An intentional, unauthorized, successful or unsuccessful breach of the facility's restricted area perimeter	○	○
An intentional, unauthorized, successful or unsuccessful breach of any critical asset's restricted area perimeter	○	○
An intentional, unauthorized, successful or unsuccessful act to either forcefully or covertly bypass, circumvent or pass through any access control point	○	○
Any incident in the vicinity of the facility or any act against the facility that requires the facility to implement additional security measures, activate procedures, or respond to with the intent of actively deterring, detecting and/ or delaying an actual threat	○	○
Any inventory control issues, product stewardship issues, theft or diversion of any chemical of interest or other dangerous chemical, tampering with any chemical of interest or any transportation container used to transport a chemical of interest, introduction of any foreign substance into any chemical of interest or into any transportation container carrying or used to carry a chemical of interest	○	○
Any act of tampering with malicious intent to cause undesirable consequences through the act itself	○	○
Any incident with malicious intent to adversely affect operations of critical cyber assets, including IT equipment used to provide security for the facility, manage processes involving chemicals of interest, or manage critical assets of the facility.	○	○
Other	○	○

If "Other" is selected, please provide a description. [Q:21.1-17005]

Training (RBPS Metric 15.1)

How often does the facility conduct training to identify the types of security incidents to report?
[Q:21.2-16945]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

How often does the facility conduct training on how to report these security incidents?
[Q:21.2-16948]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

How often does the facility conduct training on knowing to whom to report these security incidents?
[Q:21.2-16949]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

How often does the facility conduct training on knowing which facility personnel are responsible for reporting security incidents?
[Q:21.2-16950]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

How often does the facility conduct training on identifying near miss security incident reporting?
[Q:21.2-16951]

- ○ monthly
- ○ quarterly
- ○ semi-annually
- ○ annually
- ○ biennially
- ○ triennially
- ○ never

Records (RBPS Metric 15.2)

What records are maintained for security incidents?
[Q:21.3-16963]

Records	Yes	No
Access to security incident investigation reports is limited to individuals with a 'need-to-know'.	○	○
Records of security incident reports to local law enforcement/DHS are maintained in a log.	○	○
Other	○	○

If "Other" is selected, please provide a description. [Q:21.3-17008]

Near Miss (General Data Collection - RBPS 15)

How does the facility handle "near miss" security incidents?

Near Miss incidents [Q:21.4-16964]	Yes	No
Facility reviews all near miss security incidents to determine whether the near miss security incident should be reported to DHS or local law enforcement.	○	○
Facility has procedures for identifying near miss security incidents.	○	○
Other	○	○

If "Other" is selected, please provide a description. [Q:21.4-17011]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:21.88-15227]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:21.89-15235]

For more information, refer to the SSP instructions.

This page intentionally left blank.

RBPS 16 – Investigating Significant Security Incidents

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed measures for RBPS 16? [Q:22.0-18708]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 16.

Policy (RBPS Metric 16.1 and 16.2)

Indicate "Yes" for the investigation approach that apply.

How does the facility investigate significant security incidents? [Q:22.05-16692]	**Yes**	**No**
The facility has implemented a security incident investigation program to ensure that all significant security incidents within and around the facility that may have an impact on security are investigated and documented.	○	○
Significant security incidents including "near misses" are thoroughly investigated to determine their level of threat, identify vulnerability(ies) that were exploited, and determine what security upgrades, if any, are warranted to reduce the security risks.	○	○
The facility has a designated individual responsible for performing and documenting investigations of security incidents.	○	○
The facility employs a third party to perform investigations of security incidents.	○	○
The facility documents all lessons learned from security incidents.	○	○
The facility incorporates lessons learned from security incidents and investigations into employee training programs.	○	○
Other	○	○

If "Other" is selected, enter a description for the policy. [Q:22.05-16691]

Investigation (RBPS Metric 16.1)

Are incidents related to the security of the facility and materials of concern investigated to establish the details of the incident, their cause, and impacts on the security?
[Q:22.1-16693]

- ○ Yes
- ○ No
- ○ Other

If "Other" is selected, enter a description for the investigation approach. [Q:22.1-16709]

If "Yes" is selected, enter what data are collected during the investigation process.
[Q:22.1-16695]

Suggested data/facts to collect during the investigation process: Date report written, Time report written, Date reported to security official, Time reported to security official, Date of occurrence (maybe a range of dates), Time of occurrence (maybe approximate and range), Facility specific investigation/indexing case number, Location [Name of facility; Address of facility; Address of occurrence; City, State Zip Code; Regulatory site number if applicable], Person Writing Report [Name; Office location, complete address; All potential phone numbers; Fax number; Title relating to facility], Lead Investigator, all contact information, Corporate level investigator, all contact information, Type of Incident, Narrative Description of Incident, What authorities notified? [Name, title, case numbers and callback numbers of all], What compulsory notifications made? [Agency, contact person, report number], What action did the authorities take?, Were there detentions or arrests?., Where is the detainee or arrestee being housed?, List any feedback given by responding agencies, Person reporting to security [Name; Location/business address if facility related; All potential phone numbers; Title and relationship to facility], Persons of interest involved in incident [Name, Description of individuals (Clothing, Gender, Height, Approximate Weight, Race, Nationality, passport, visa information if appropriate, Hair color, Eye color, Approximate Age, Any other unique characteristics, ID numbers, etc., Contact made by police?); What is the apparent intent/activity of the individual?; Did they take photographs, make drawings, take video images (Disposition of above); Did they make any statements? Describe.; Did they ask for information they did not have a need to know about?; Vehicles (License plate number and state, Make, Model, Year, Color, Type, Other unique descriptors, Direction of Travel, Contact made by police?)], Witnesses [Name; Location/address; Relationship to facility; All available phone numbers], Prosecutions involved? [Agency prosecuting, Contact information], Formal internal investigation date completed, Action items from investigation, Action items responsible parties identified, Completion dates for action items, Review of effectiveness of action items, Other facts/data

Investigator Qualifications (RBPS Metric 16.1)

Indicate "Yes" for the investigator qualifications that apply.

What are the qualifications of incident investigators utilized by the facility? [Q:22.2-16870]	**Yes**	**No**
Facility uses local police to investigate security incidents.	○	○
Facility uses a private investigator to investigate security incidents.	○	○
Facility uses a police detective to investigate security incidents.	○	○
Facility uses a member of its security staff to investigate security incidents.	○	○
Other	○	○

If "Other" is selected, enter a description for the investigator qualifications. [Q:22.2-16873]

Investigation Lesson Learned (RBPS Metric 16.2)

Does the facility identify, compile, and document lessons learned from its security incident investigation program?
[Q:22.3-16877]

○ Yes
○ No

Does the facility disseminate lessons learned from its security incident investigation program to its employees?
[Q:22.3-16879]

○ Yes
○ No
○ Other

If "No" is selected, go to Planned Measures.

If "Other" is selected, enter a description for the investigation lesson learned approach.
[Q:22.3-16881]

Investigation Lesson Learned Present (RBPS Metric 16.2)

Does the facility disseminate lessons learned from its security incident investigation program before or as part of the next training session where the lessons learned apply?
[Q:22.31-16888]

- ○ Yes
- ○ No

What instructional methods does the facility employ to disseminate lessons learned from its security incident investigation program?
[Q:22.31-16891]

- ○ Hands-on activities
- ○ Hand-outs, bulletin boards, etc.
- ○ Lectures
- ○ On-line or interactive programs
- ○ Orientations
- ○ Seminars
- ○ Workshops
- ○ Briefings
- ○ Video
- ○ Other

If "Other" is selected, enter a description for the investigation lesson learned approach.
[Q:22.31-16912]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:22.88-15228]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:22.89-15236]

For more information, refer to the SSP instructions.

RBPS 17 – Officials and Organization

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 17? [Q:23.0-18707]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 17.

Policy (RBPS Metrics 17.1, 17.2, 17.4, and 17.5)

Describe the security organization of the facility.

Policy [Q:23.05-16341]	**Yes**	**No**
The facility has defined a security organizational structure in writing that identifies specific security duties and responsibilities.	○	○
The facility SSP includes the names, contact information and responsibilities of security officials included in the security organizational structure.	○	○
The company or corporation has more than one facility subject to CFATS, and has designated a Corporate Security Officer (CSO) to coordinate security at a corporate level.	○	○
The facility has designated a Site Security Officer (SSO) to lead the implementation of the CFATS on a facility level.	○	○
Facility has designated a Cyber Security Officer to be in charge of cyber security issues at the facility.	○	○
The facility has designated an Alternate SSO to function in place of the SSO should circumstances dictate.	○	○
Facility has a procedure in place (officials change management policy) for updating its SSP to reflect changes in personnel when turnover occurs for the CSO, SSO, Alternate SSO, Cyber SO, and Facility Plant manager positions.	○	○
Facility maintains an Audit Log documenting the dates and reasons for changes in personnel for the CSO, SSO, Alternate SSO, Cyber SO, and Facility Plant manager positions.	○	○
The facility has an emergency and security response organization and program to respond to site emergencies and security events.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:23.05-17012]

SSO Responsibilities (RBPS Metric 17.3)

What are the responsibilities of the Site Security Officer (SSO)?

SSO Responsibilities [Q:23.1-16365]	**Yes**	**No**
The SSO is responsible for ensuring that individuals assigned to the security organization discharge their duties appropriately.	○	○
The SSO is responsible for conducting and supervising the submission of the Security Vulnerability Assessment.	○	○
The SSO is responsible for hosting DHS inspections.	○	○
The SSO is responsible for designing and documenting security training for all employees to include security awareness of all personnel.	○	○
The SSO is responsible for maintaining records, as required by the CFATS.	○	○
The SSO is responsible for planning and documenting of security drills and exercises.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:23.1-17013]

SSO Qualifications (General Data Collection - RBPS 17)

What are the qualifications of the Site Security Officer (SSO)?

Qualifications [Q:23.2-16366]	**Yes**	**No**
SSO understands the facility security organization.	○	○
SSO understands the facility's requirement to comply with the CFATS RBPS.	○	○

Qualifications [Q:23.2-16366]	**Yes**	**No**
SSO has experience in emergency preparedness, response and planning for disasters.	○	○
SSO is familiar with responsibilities and functions of local, State and Federal law enforcement agencies.	○	○
SSO has ability to recognize characteristics and behavioral patterns of persons likely to threaten security.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:23.2-17016]

Security Organization (General Data Collection - RBPS 17)

Has a security organization been established for the protection of the facility? [Q:23.3-16872]

○ Yes

○ No

If "No" is selected, go to Planned Measures.

Select "Yes", if applicable

Security Organization (General Data Collection – RBPS 17) [Q:23.31-16874]	**Yes**	**No**
A security organization has been established for the protection of the facility.	○	○
The security organization's primary responsibility is to provide protection of the facility's assets, including personnel, facilities and equipment, and materials of interest.	○	○
The security organization has a documented and current chain of command, included in the SSP.	○	○
A security management organization exists to develop, revise, and implement security policies and procedures at the facility.	○	○
The security organization has identified interface structure with facility operations.	○	○
The facility plant manager assists the Site Security Officer by ensuring cooperation of facility plant personnel with the requirements of the SSP and CFATS as it applies to them	○	○
A proprietary security is maintained as the security organization for the facility.	○	○

Security Organization (General Data Collection – RBPS 17) [Q:23.31-16874]	**Yes**	**No**
A contract security is maintained as the security organization for the facility.	○	○
The security organization employs unarmed security personnel.	○	○
The security organization employs armed security personnel.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:23.31-17026]

What is the status of the security organization for the facility? [Q:23.31-16875]

○ Proprietary
○ Contract
○ Other

If "Other" is selected, enter a description: [Q:23.31-17040]

Does the security organization employ armed security personnel? [Q:23.31-16876]

○ Yes
○ No

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:23.88-15229]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:23.89-15237]

For more information, refer to the SSP instructions.

RBPS 18 – Records

Please be sure you are familiar with this RBPS, the SSP instructions and RBPS Guidance before answering this question.

Does the facility have any existing, planned, or proposed security measures for RBPS 18? [Q:24.0-18708]

- ○ Yes
- ○ No

If "No" is selected, skip the rest of RBPS 18.

Training (RBPS Metric 18.1)

How many years does the facility retain training records, in paper or electronic format? [Q:24.005-14514] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility include with each training record?

Training Records [Q:24.005-14645]	**Yes**	**No**	**Other**
Date and location of each se	○	○	○
Time of day and duration of session	○	○	○
Description of the training	○	○	○
Name and qualifications of the instructor	○	○	○
Clear, legible list of attendees to include the attendee signature, at least one other unique identifier or each attendee receiving the training	○	○	○
Results of any evaluation or testing	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.005-14524]

Drills/Exercises (RBPS Metric 18.2)

How many years does the facility retain records of drills and exercises, in paper or electronic format? [Q:24.01-14544] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility include with each drill/exercise record?

Drills/Exercises [Q:24.01-14646]	**Yes**	**No**	**Other**
Date held	○	○	○
Description of the drill or exercise	○	○	○
List of participants	○	○	○
List of equipment (other than personal equipment) tested or employed in the exercise	○	○	○
Name(s) and qualifications of the exercise director	○	○	○
Best practices or lessons learned which may improve the Site Security Plan	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.01-14546]

Incidents and Breaches of Security (RBPS Metric 18.3)

How many years does the facility retain records of incidents and breaches of security, in paper or electronic format? [Q:24.02-14550] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility include with each incident/breach record?

Incidents and Breaches [Q:24.02-14647]	**Yes**	**No**	**Other**
Date and time of occurrence	○	○	○

Incidents and Breaches [Q:24.02-14647]	**Yes**	**No**	**Other**
Location within the facility	○	○	○
Description of the incident or breach	○	○	○
Identity of the individual to whom it was reported	○	○	○
Description of the response	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.02-14552]

Maintenance/Testing (RBPS Metric 18.4)

How many years does the facility retain records of maintenance, calibration, and testing of security equipment, in paper or electronic format? [Q:24.03-14563] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility include with each record of maintenance, calibration, and testing of security equipment?

Incidents and Breaches [Q:24.03-14650]	**Yes**	**No**	**Other**
Date and time	○	○	○
Name and qualifications of the technician(s) doing the work	○	○	○
Specific security equipment involved for each occurrence of maintenance, calibration ,and testing	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.03-14565]

Security Threats (RBPS Metric 18.5)

How many years does the facility retain records of security threats, in paper or electronic format? [Q:24.04-14557] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility include with each threat record?

Security Threats [Q:24.04-14648]	**Yes**	**No**	**Other**
Date and time of occurrence	○	○	○
How the threat was communicated	○	○	○
Who received or identified the threat	○	○	○
Description of the threat	○	○	○
To whom it was reported	○	○	○
Description of the response	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.04-14559]

Audits (RBPS Metric 18.6)

How many years does the facility retain audit records, in paper or electronic format? [Q:24.05-14560] (Choose one: 3 or more years, 2 years, 1 year, None).

What information does the facility retain with each audit of a covered facility's Site Security Plan or Security Vulnerability Assessment?

Audits [Q:24.05-14649]	**Yes**	**No**	**Other**
A record of the audit	○	○	○

Audits [Q:24.05-14649]	**Yes**	**No**	**Other**
Results of the audit	○	○	○
Name(s) of the person(s) who conducted the audit	○	○	○
A letter certified by the covered facility stating the date the audit was conducted	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.05-14562]

DHS Correspondence (RBPS Metric 18.7)

How many years does the facility retain all Letters of Authorization and Approval from the Department, and documentation identifying the results of audits and inspections conducted pursuant to §27.250, in paper or electronic format? [Q:24.08-14566] (Choose one: 3 or more years, 2 years, 1 year, None).

CSAT Documentation (RBPS Metric 18.8)

How many years does the facility retain records of submitted Top-Screens, Security Vulnerability Assessments, Site Security Plans, and all related correspondence with the Department, in paper or electronic format? [Q:24.08-14567] (Choose one: 0 years, < 6 years, 6 years, > 6 years).

SSP/ASP Documentation (RBPS Metric 18.9)

How many years does the facility retain records related to an Alternative Security Program which is submitted in lieu of a Security Vulnerability Assessment or a Site Security Plan pursuant to §27.235? [Q:24.08-14568] (Choose one: 0 years, < 6 years, 6 years, > 6 years).

RBPS 18 - General Data Collection

What access control records does the facility maintain?

Access Control [Q:24.09-14754]	**Yes**	**No**	**Other**
A record of all individuals authorized access to the facility is maintained.	○	○	○
A record of all individuals authorized access to the restricted areas of the facility is maintained.	○	○	○
A register of all visitors, vendors, etc. to the facility is maintained	○	○	○
Records of federal, state and local officials authorized access are maintained.	○	○	○
Other	○	○	○

If "Other" is selected, enter a description: [Q:24.09-14595]

Records Administration - Creation

Does facility prepare a detailed written account or record for training; drills and exercises; incidents and breaches of security; maintenance, calibration, and testing of security equipment; security threats or similar incidents? [Q:24.1-14619]

○ Yes
○ No
○ Other

If "No" is selected, go to Planned Measures.

If "Other" is selected, enter a description: [Q:24.1-22798]

What records or detailed written accounts does the facility prepare?

Records Creation [Q:24.11-14755]	**Yes**	**No**
Training	○	○
Drills and exercises	○	○
Incidents and breaches of security	○	○
Maintenance, calibration, and testing of security equipment	○	○
Security threats	○	○
Audits of Site Security Plans (including audits required under 6 CFR § 27.225(e)) and Security Vulnerability Assessments	○	○
Letters of authorization and approval from DHS	○	○
Documentation identifying the results of audits and inspections conducted pursuant to 6 CFR §27.250	○	○
Submitted Top-Screens	○	○
Submitted Security Vulnerability Assessments	○	○
Submitted Site Security Plans	○	○
All related correspondence with the DHS	○	○

Records Administration - Maintenance

What records or detailed written accounts does the facility maintain?

Records Maintenance [Q:24.12-14756]	**Yes**	**No**
Facility maintains written records in electronic format.	○	○
Facility maintains written records in paper format.	○	○
Facility maintains written records in a location that is accessible.	○	○
Facility ensures that written records are not disposed of before the time period for their retention has elapsed.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:24.12-22798]

Does the facility maintain and protect written records in accordance with 6 CFR Part 27.255 and/or provisions regarding Chemical-terrorism Vulnerability Information (CVI), 6 CFR Part 27.400? [Q:24.12-14621]

- ○ Yes
- ○ No

Records Administration - Storage

How are records stored in the facility?

Records Storage [Q:24.13-14757]	**Yes**	**No**
Facility stores records in an appropriate and accessible location.	○	○
Facility storage location is known to the facility personnel, should records need to be retrieved for a DHS inspection.	○	○
Facility storage location is kept locked with more than one person able to access the records in order to produce records for a DHS inspection.	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:24.13-14625]

Records Administration - Disposal

How are records disposed in the facility?

Records Disposal [Q:24.14-14758]	**Yes**	**No**
Facility disposes of the written record in accordance with 6 CFR Part 27.255 and/or provisions regarding Chemical-terrorism Vulnerability Information (CVI), 6 CFR Part 27.400.	○	○
Facility destroys written records covered by CVI, 6 CFR Part 27.400, in accordance with 6 CFR Part 27.400(k).	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:24.14-14628]

Records Administration - Availability

Can the facility produce records for examination and copying by DHS within a reasonable period of time? [Q:24.15-14629]

○ Yes

○ No

If "No" is selected, go to Planned Measures.

Records Administration - Availability of Records

Are records available for examination and copying at the facility?

Availability of Records [Q:24.16-14759]	**Yes**	**No**
Facility can produce CFATS required records for examination and copying by DHS within 4 hours for a scheduled inspection.	○	○
Facility can produce CFATS required records for examination and copying by DHS within a reasonable period of time for an unscheduled inspection.	○	○
Facility can produce additional CFATS relevant records necessary for security purposes kept pursuant to other Federal programs or regulations, see 6 CFR Part 27.255 (c).	○	○
Other	○	○

If "Other" is selected, enter a description: [Q:24.16-14631]

Planned Measures

Describe any planned security measures that the facility wants DHS to consider in determining the satisfaction of the RBPS. [Q:24.88-14765]

For more information, refer to the SSP instructions.

Proposed Measures

Does the facility have any proposed security measures for satisfying this RBPS that it wants to share with DHS? In the response to this question, the facility may share with DHS any existing or planned security measures the facility proposes to remove or eliminate to include a general timeline for such action. In the response to this question, the facility may also identify any existing or planned security measures which the facility has identified in this RBPS section, but which the facility does not wish DHS to include in evaluating its SSP for approval. Please see section 4.1.3 and 5.1.3 of the CSAT Site Security Plan Instructions for more detail. [Q:24.89-14766]

For more information, refer to the SSP instructions.