The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Chemical Sector Suspicious Activity Reporting Tool Overview

2012 Chemical Sector Security Summit

July 31, 2012

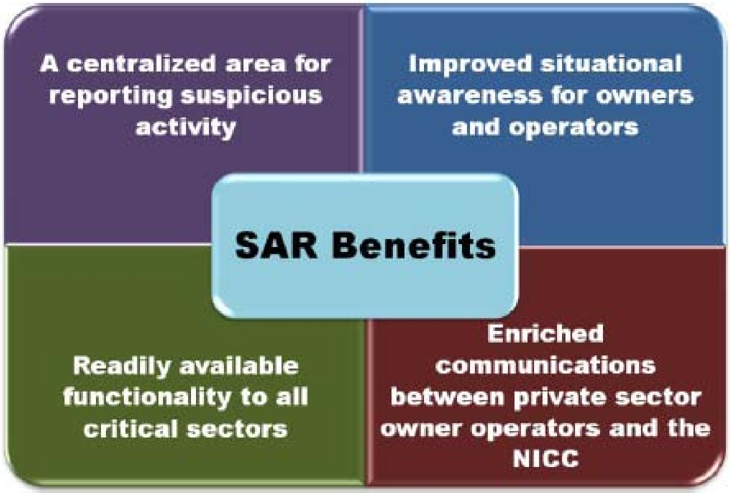
Homeland Security

Agenda

- Suspicious Activity Reporting (SAR) Pilot Program Background and Purpose
- SAR Tool on HSIN-CS
- SAR Tool Demonstration
- Question & Answer Session

SAR Pilot Program Background and Purpose

- In support of the "If You See Something, Say Something™" initiative, the Department's National Protection and Programs Directorate, Office of Infrastructure Protection (NPPD/IP) developed a standardized means by which Critical Infrastructure (CI) stakeholders across all 18 CI sectors can report suspicious activities to the government via the Homeland Security Information Network/Critical Sectors (HSIN-CS)
- The SAR tool facilitates consistent submission and processing of Suspicious Activity Reports, efficient information sharing, and responsiveness
- February - June 2011, the Commercial Facilities and Highway and Motor Carrier sectors participated in a pilot on HSIN-CS
- The HSIN-CS SAR Tool was rolled out to the Chemical, Commercial Facilities, Dams, and Highway Motor Carrier Sectors
- Roll-out to additional sectors, Summer 2012


SAR Benefits

A centralized area for reporting suspicious activity

Improved situational awareness for owners and operators

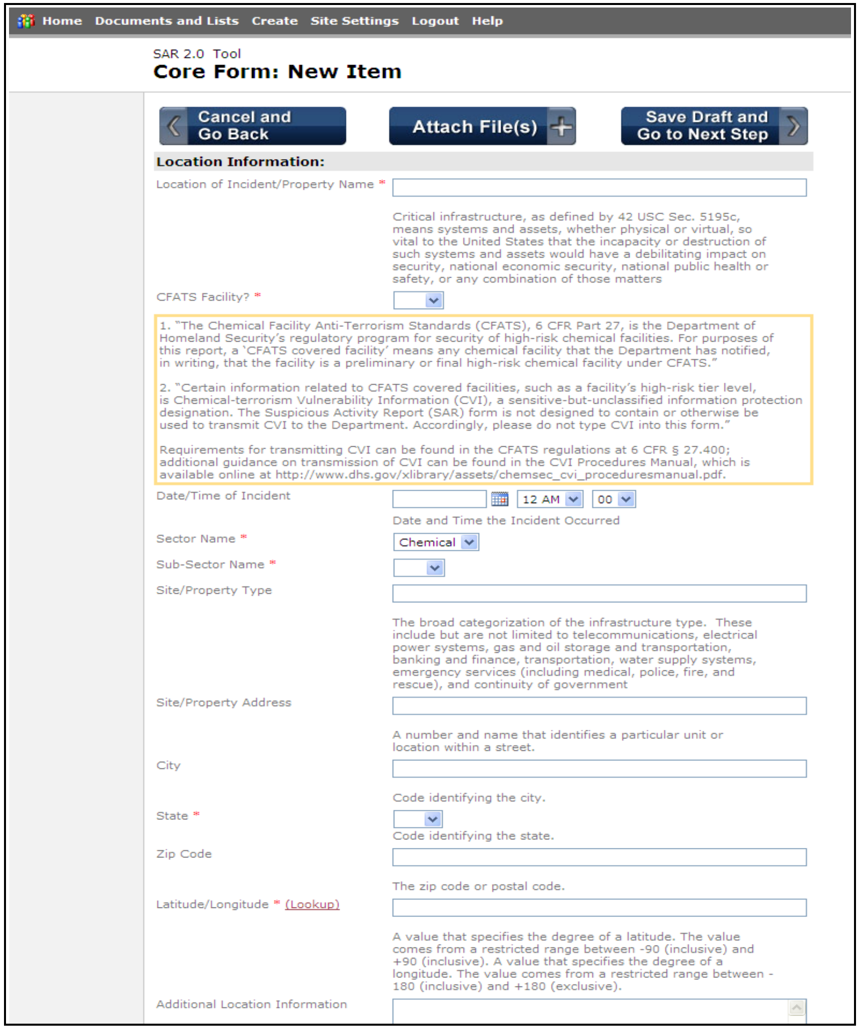
Readily available functionality to all critical sectors

Enriched communications between private sector owner operators and the NICC

Figure 1: DHS

Homeland Security

SAR Tool on HSIN-CS



SAR 2.0 Tool

Core Form: New Item

Location Information:

Location of Incident/Property Name *

Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters

CFATS Facility? *

1. "The Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, is the Department of Homeland Security's regulatory program for security of high-risk chemical facilities. For purposes of this report, a 'CFATS covered facility' means any chemical facility that the Department has notified, in writing, that the facility is a preliminary or final high-risk chemical facility under CFATS."

2. "Certain information related to CFATS covered facilities, such as a facility's high-risk tier level, is Chemical-terrorism Vulnerability Information (CVI), a sensitive-but-unclassified information protection designation. The Suspicious Activity Report (SAR) form is not designed to contain or otherwise be used to transmit CVI to the Department. Accordingly, please do not type CVI into this form."

Requirements for transmitting CVI can be found in the CFATS regulations at 6 CFR § 27.400; additional guidance on transmission of CVI can be found in the CVI Procedures Manual, which is available online at http://www.dhs.gov/xlibrary/assets/chemsec_cvi_proceduresmanual.pdf.

Date/Time of Incident: 12 AM 00

Date and Time the Incident Occurred

Sector Name *: Chemical

Sub-Sector Name *

Site/Property Type

The broad categorization of the infrastructure type. These include but are not limited to telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government

Site/Property Address

A number and name that identifies a particular unit or location within a street.

City

Code identifying the city.

State *

Code identifying the state.

Zip Code

The zip code or postal code.

Latitude/Longitude * (Lookup)

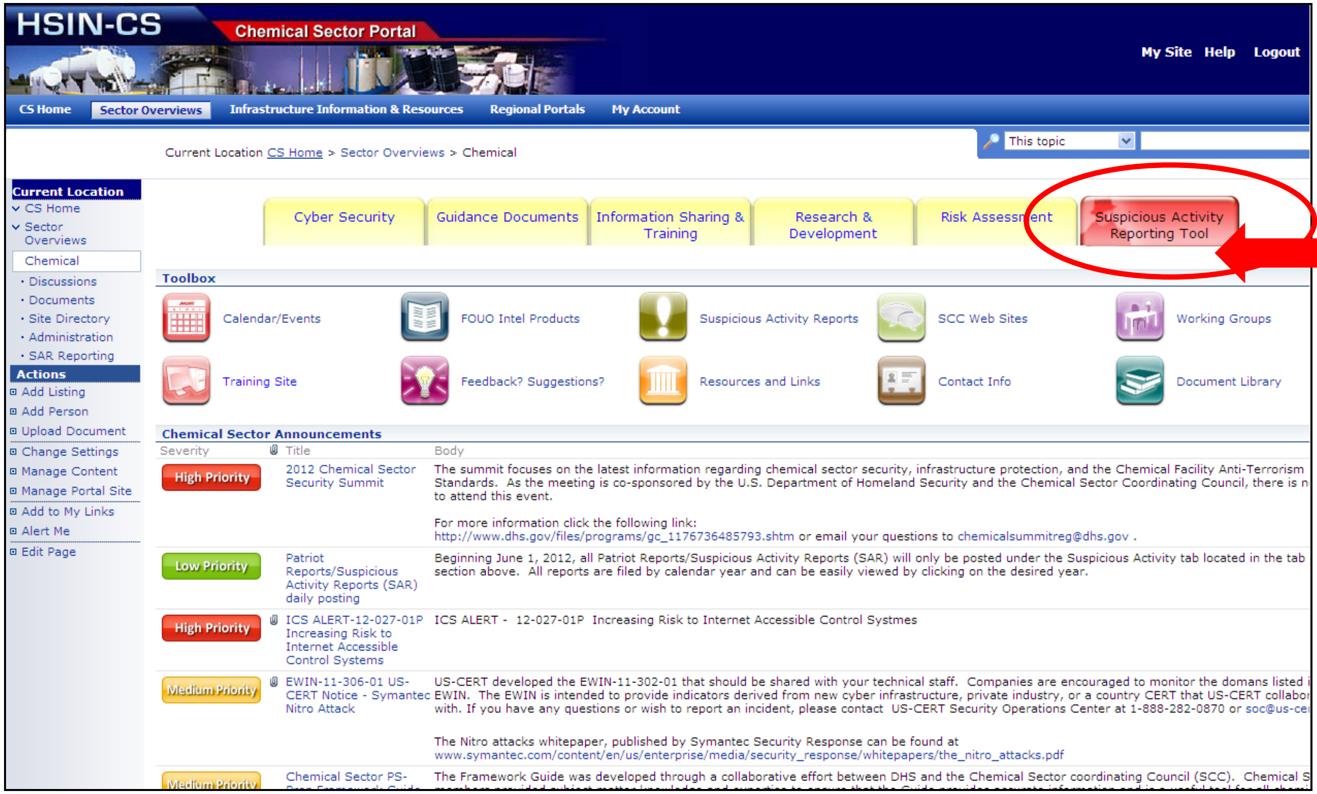
A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive). A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).

Additional Location Information

Figure 2: DHS

- The HSIN-CS SAR form is aligned with the National SAR Initiative's (NSI's) emerging standards and contains National Information Exchange Model (NIEM)-compliant fields and dropdown lists.
- Dynamic SAR form allows the submitter to provide information on relevant supplemental forms
- Core Form contains 3 primary sections:
  - Location Information
  - Incident Information
  - Submitter Information
- Supplemental forms include:
  - Observer(s)
  - Witness(es)
  - Individual(s) Involved
  - Vehicle(s)
  - Aircraft(s)
  - Vessel(s)

HSIN-Chemical Homepage Page



SAR Tool

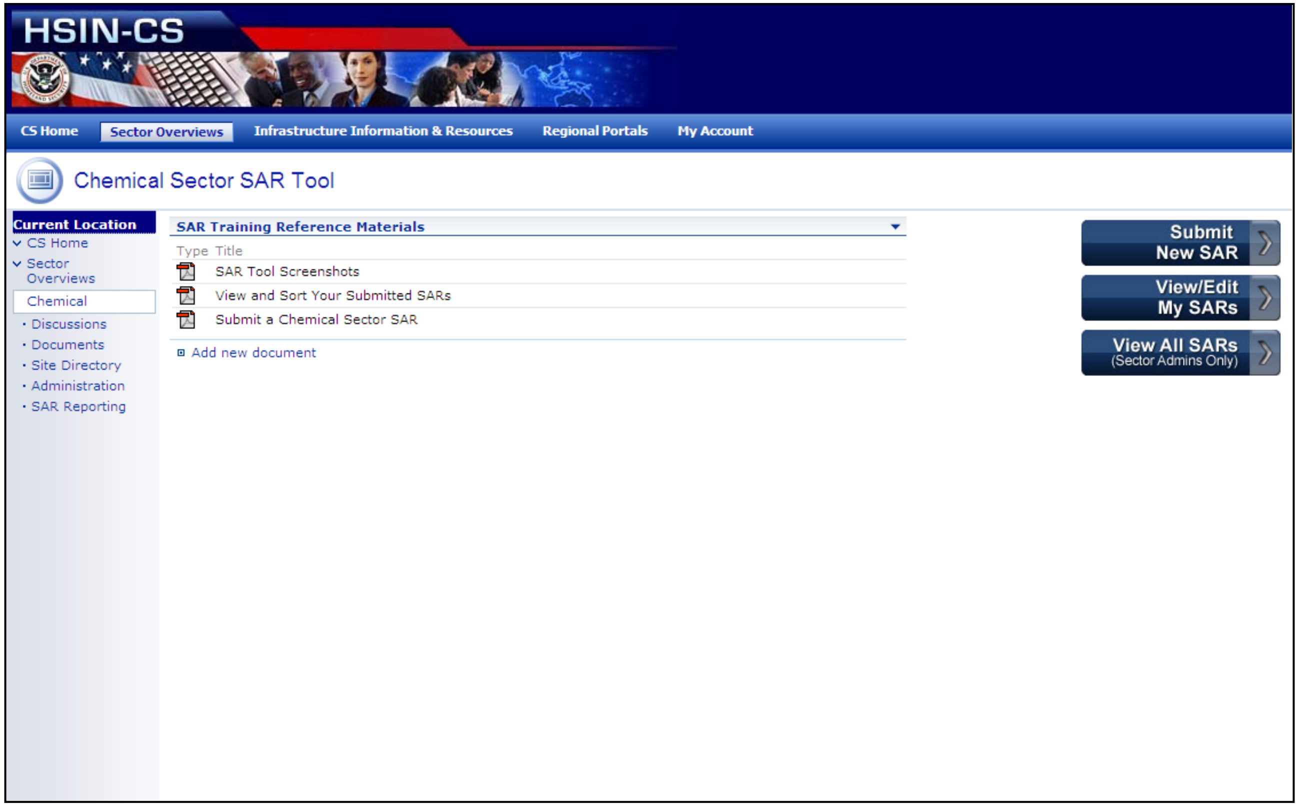
Chemical Sector Announcements

Severity	Title	Body
High Priority	2012 Chemical Sector Security Summit	The summit focuses on the latest information regarding chemical sector security, infrastructure protection, and the Chemical Facility Anti-Terrorism Standards. As the meeting is co-sponsored by the U.S. Department of Homeland Security and the Chemical Sector Coordinating Council, there is n to attend this event. For more information click the following link: http://www.dhs.gov/files/programs/gc_1176736485793.shtm or email your questions to chemicalsummitreg@dhs.gov .
Low Priority	Patriot Reports/Suspicious Activity Reports (SAR) daily posting	Beginning June 1, 2012, all Patriot Reports/Suspicious Activity Reports (SAR) will only be posted under the Suspicious Activity tab located in the tab section above. All reports are filed by calendar year and can be easily viewed by clicking on the desired year.
High Priority	ICS ALERT-12-027-01P Increasing Risk to Internet Accessible Control Systems	ICS ALERT - 12-027-01P Increasing Risk to Internet Accessible Control Systmes
Medium Priority	EWIN-11-306-01 US-CERT Notice - Symantec Nitro Attack	US-CERT developed the EWIN-11-302-01 that should be shared with your technical staff. Companies are encouraged to monitor the domans listed i EWIN. The EWIN is intended to provide indicators derived from new cyber infrastructure, private industry, or a country CERT that US-CERT collabor with. If you have any questions or wish to report an incident, please contact US-CERT Security Operations Center at 1-888-282-0870 or soc@us-ce The Nitro attacks whitepaper, published by Symantec Security Response can be found at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
Medium Priority	Chemical Sector PS-	The Framework Guide was developed through a collaborative effort between DHS and the Chemical Sector coordinating Council (SCC). Chemical S

Figure 3: DHS

Homeland Security

SAR Tool Landing Page



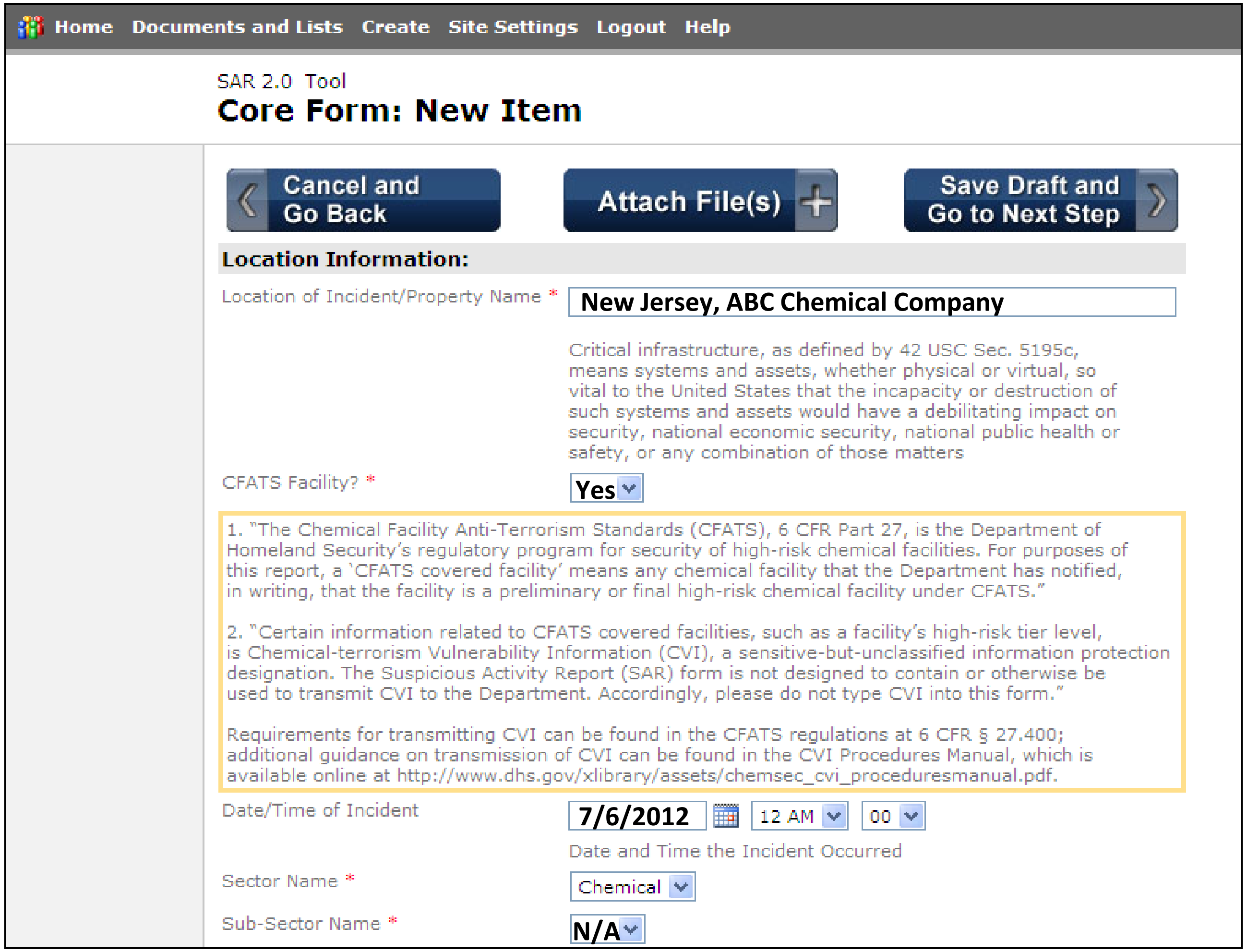
Chemical Sector SAR Tool

SAR Training Reference Materials

Type	Title
	SAR Tool Screenshots
	View and Sort Your Submitted SARs
	Submit a Chemical Sector SAR

Figure 4: DHS

Core Form: Location Information



Home Documents and Lists Create Site Settings Logout Help

SAR 2.0 Tool

Core Form: New Item

Cancel and Go Back
Attach File(s)
Save Draft and Go to Next Step

Location Information:

Location of Incident/Property Name * New Jersey, ABC Chemical Company

Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters

CFATS Facility? * Yes

1. "The Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, is the Department of Homeland Security's regulatory program for security of high-risk chemical facilities. For purposes of this report, a 'CFATS covered facility' means any chemical facility that the Department has notified, in writing, that the facility is a preliminary or final high-risk chemical facility under CFATS."

2. "Certain information related to CFATS covered facilities, such as a facility's high-risk tier level, is Chemical-terrorism Vulnerability Information (CVI), a sensitive-but-unclassified information protection designation. The Suspicious Activity Report (SAR) form is not designed to contain or otherwise be used to transmit CVI to the Department. Accordingly, please do not type CVI into this form."

Requirements for transmitting CVI can be found in the CFATS regulations at 6 CFR § 27.400; additional guidance on transmission of CVI can be found in the CVI Procedures Manual, which is available online at http://www.dhs.gov/xlibrary/assets/chemsec_cvi_proceduresmanual.pdf.

Date/Time of Incident 7/6/2012 12 AM 00

Date and Time the Incident Occurred

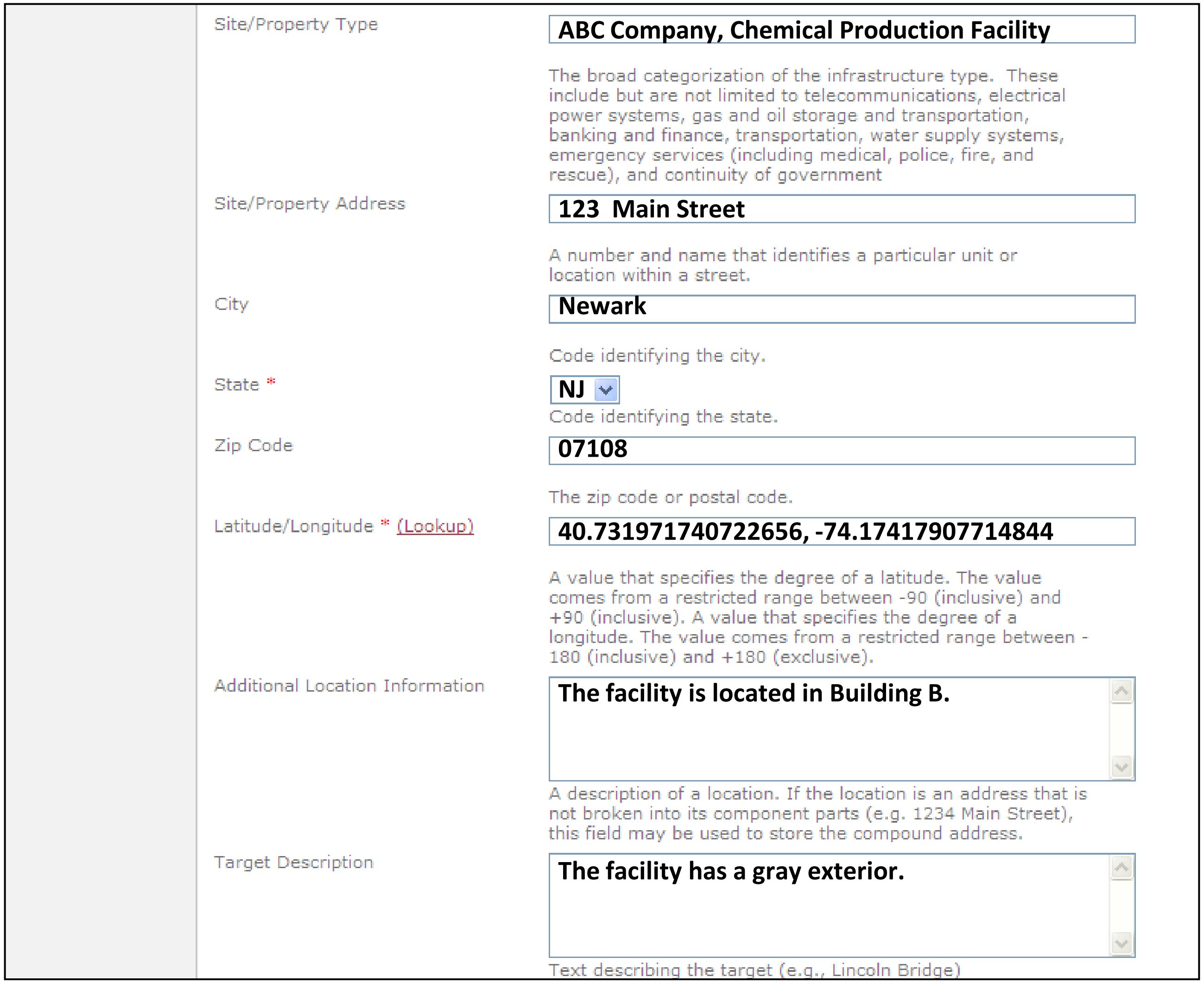
Sector Name * Chemical

Sub-Sector Name * N/A

Figure 5: DHS

Homeland Security

Core Form: Location Information (cont.)



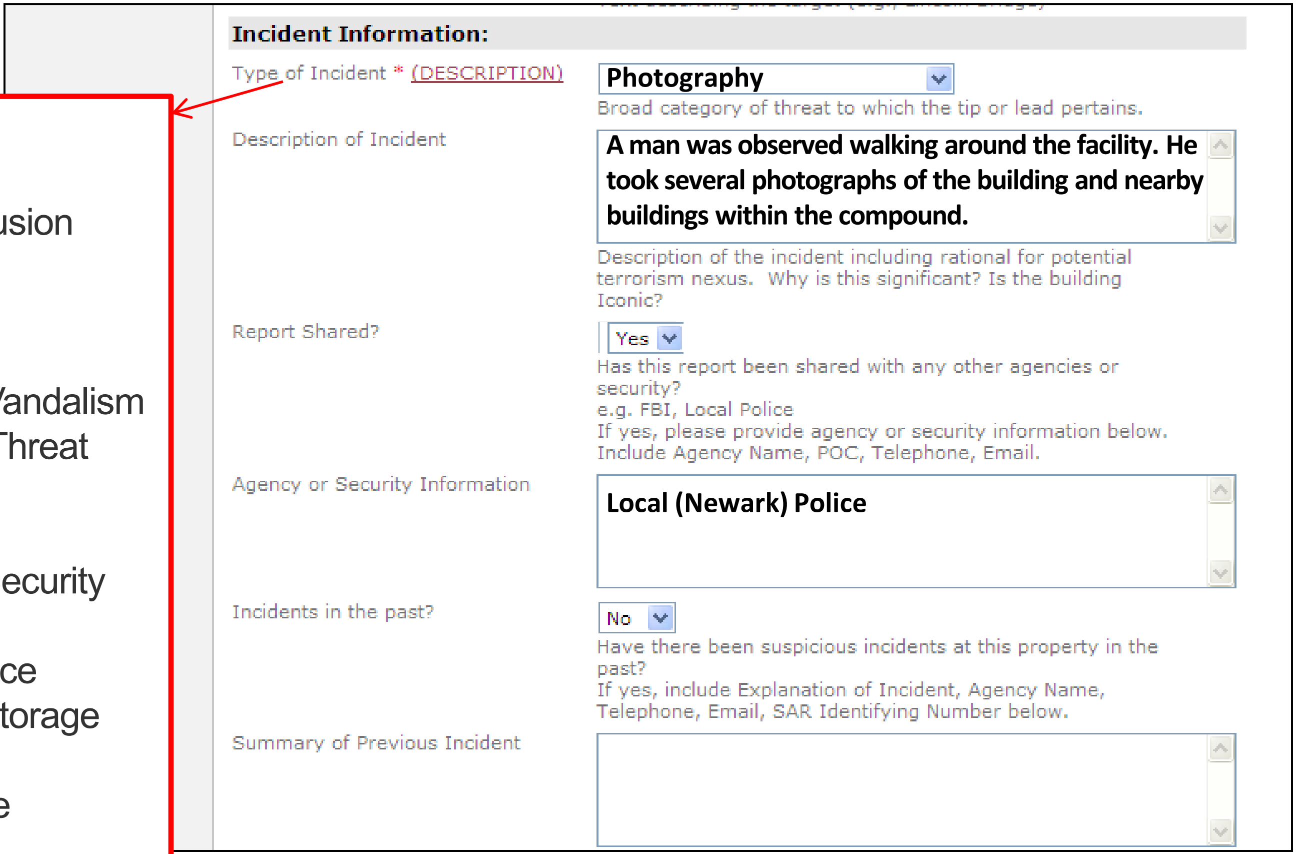
Site/Property Type	ABC Company, Chemical Production Facility The broad categorization of the infrastructure type. These include but are not limited to telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government
Site/Property Address	123 Main Street A number and name that identifies a particular unit or location within a street.
City	Newark Code identifying the city.
State *	NJ Code identifying the state.
Zip Code	07108 The zip code or postal code.
Latitude/Longitude * (Lookup)	40.731971740722656, -74.17417907714844 A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive). A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
Additional Location Information	The facility is located in Building B. A description of a location. If the location is an address that is not broken into its component parts (e.g. 1234 Main Street), this field may be used to store the compound address.
Target Description	The facility has a gray exterior. Text describing the target (e.g., Lincoln Bridge)

Figure 6: DHS

Core Form: Incident Information

Types of Incidents

- Breach/Attempted Intrusion
- Misrepresentation
- Theft/Loss/Diversion
- Cyber Attack
- Sabotage/Tampering/Vandalism
- Expressed or Implied Threat
- Aviation Activity
- Eliciting Information
- Testing or Probing of Security
- Photography
- Observation/Surveillance
- Materials Acquisition/Storage Acquisition
- Acquisition of Expertise
- Weapons Discovery
- Sector-Specific Incident



Incident Information:

Type of Incident * (DESCRIPTION): **Photography**
Broad category of threat to which the tip or lead pertains.

Description of Incident: **A man was observed walking around the facility. He took several photographs of the building and nearby buildings within the compound.**
Description of the incident including rational for potential terrorism nexus. Why is this significant? Is the building Iconic?

Report Shared?: Yes
Has this report been shared with any other agencies or security?
e.g. FBI, Local Police
If yes, please provide agency or security information below.
Include Agency Name, POC, Telephone, Email.

Agency or Security Information: **Local (Newark) Police**

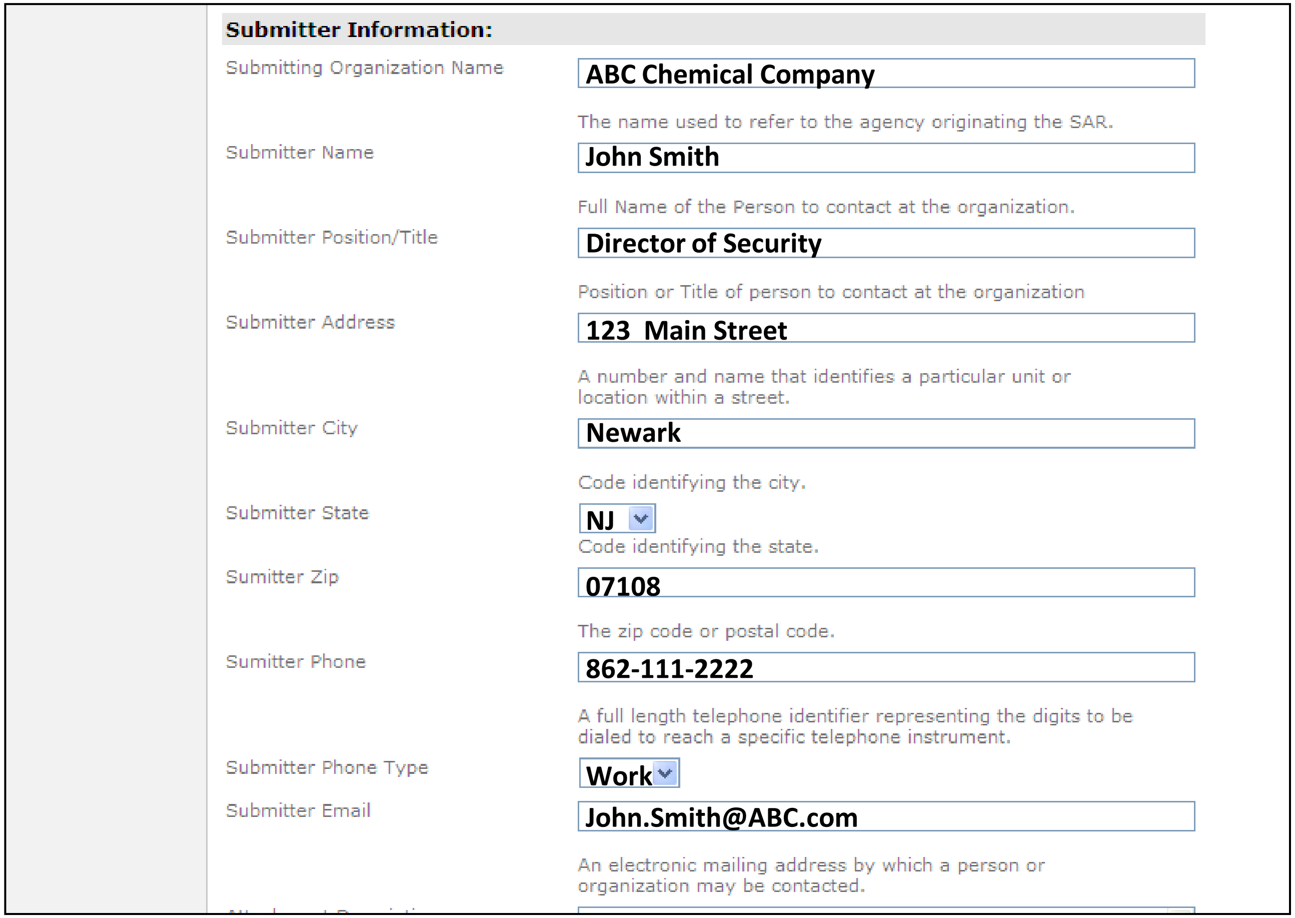
Incidents in the past?: No
Have there been suspicious incidents at this property in the past?
If yes, include Explanation of Incident, Agency Name, Telephone, Email, SAR Identifying Number below.

Summary of Previous Incident:

Figure 7: DHS

Homeland Security

Core Form: Submitter Information



Submitter Information:

Submitting Organization Name: ABC Chemical Company
The name used to refer to the agency originating the SAR.

Submitter Name: John Smith
Full Name of the Person to contact at the organization.

Submitter Position/Title: Director of Security
Position or Title of person to contact at the organization

Submitter Address: 123 Main Street
A number and name that identifies a particular unit or location within a street.

Submitter City: Newark
Code identifying the city.

Submitter State: NJ
Code identifying the state.

Sumitter Zip: 07108
The zip code or postal code.

Sumitter Phone: 862-111-2222
A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument.

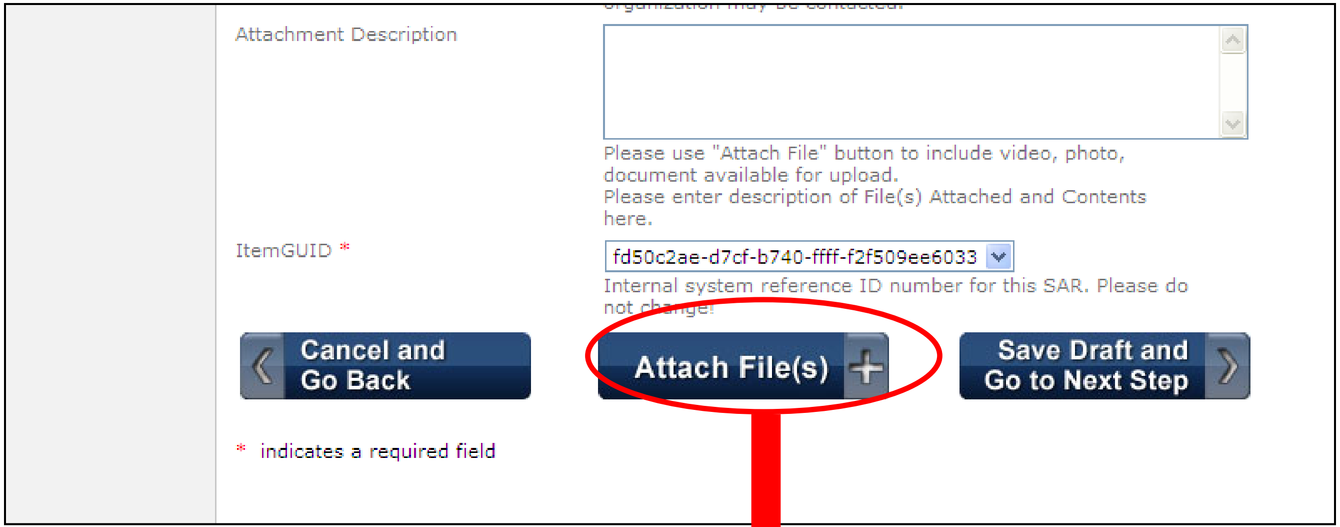
Submitter Phone Type: Work

Submitter Email: John.Smith@ABC.com
An electronic mailing address by which a person or organization may be contacted.

Figure 8: DHS

Homeland Security

Core Form: Attaching File(s)



organization may be contacted.

Attachment Description

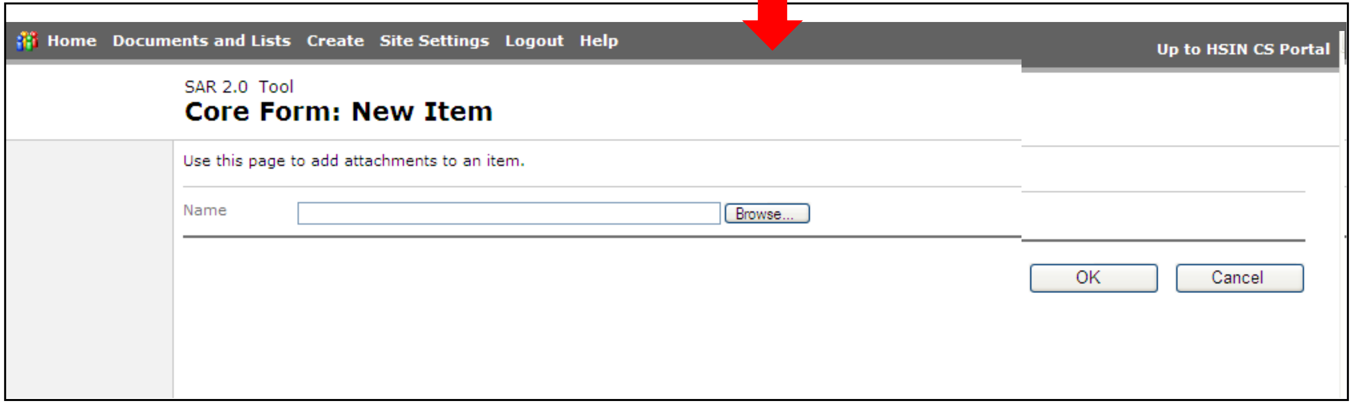
Please use "Attach File" button to include video, photo, document available for upload.
Please enter description of File(s) Attached and Contents here.

ItemGUID *

fd50c2ae-d7cf-b740-ffff-f2f509ee6033

Internal system reference ID number for this SAR. Please do not change!

* indicates a required field



SAR 2.0 Tool

Core Form: New Item

Use this page to add attachments to an item.

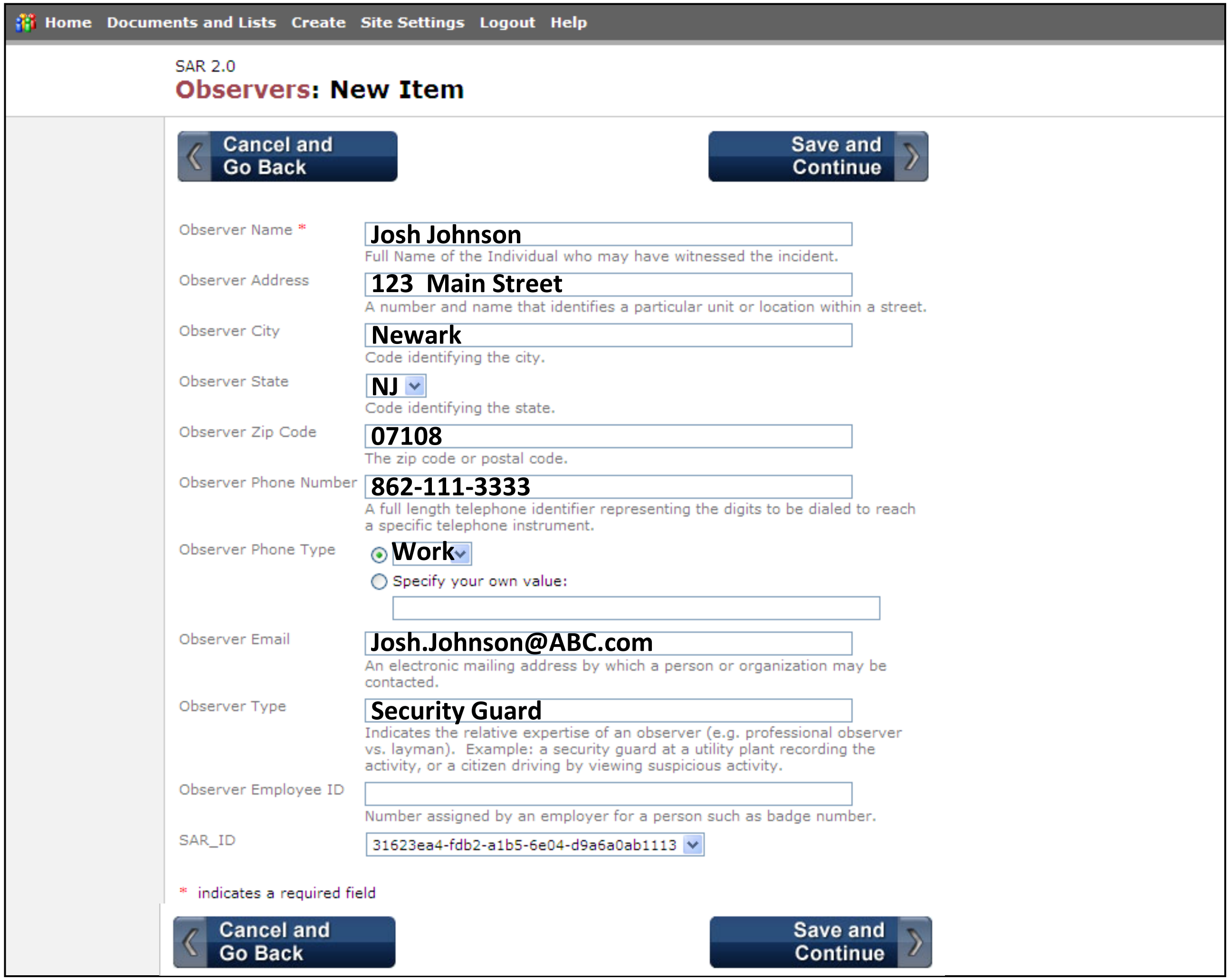
Name

Accepted File Types for Attachment(s): PDF, PPT, PPTX, DOC, DOCX, XLS, XLSX, JPEG, BMP, TIF, PUB, MOV, WMV, FLV, MP3, WAV, MPEG

Figure 9: DHS

Homeland Security

Supplemental Form: Observer(s)



SAR 2.0

Observers: New Item

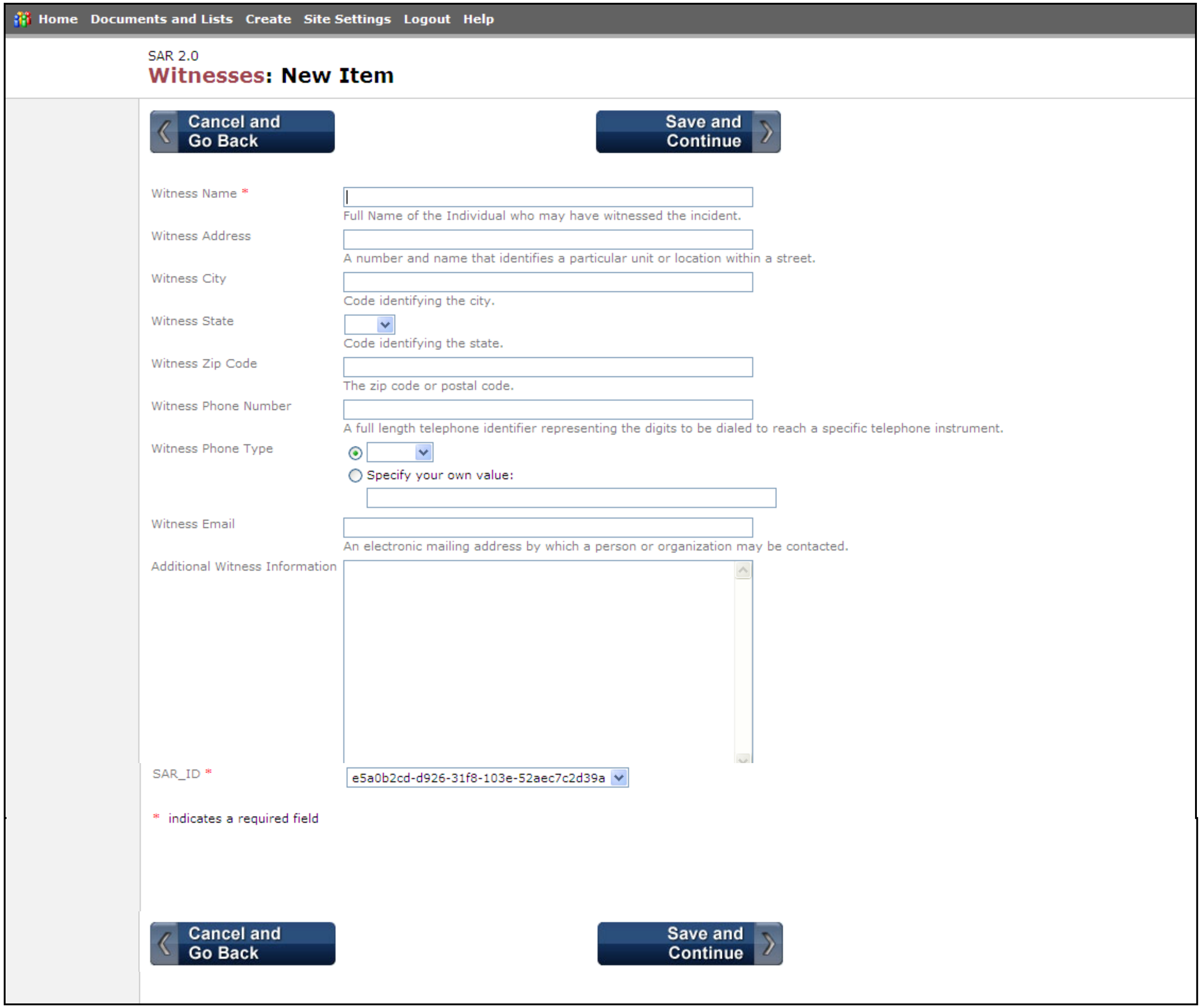
Observer Name *	Josh Johnson Full Name of the Individual who may have witnessed the incident.
Observer Address	123 Main Street A number and name that identifies a particular unit or location within a street.
Observer City	Newark Code identifying the city.
Observer State	NJ Code identifying the state.
Observer Zip Code	07108 The zip code or postal code.
Observer Phone Number	862-111-3333 A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument.
Observer Phone Type	● Work ○ Specify your own value:
Observer Email	Josh.Johnson@ABC.com An electronic mailing address by which a person or organization may be contacted.
Observer Type	Security Guard Indicates the relative expertise of an observer (e.g. professional observer vs. layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity.
Observer Employee ID	Number assigned by an employer for a person such as badge number.
SAR_ID	31623ea4-fdb2-a1b5-6e04-d9a6a0ab1113

* indicates a required field

Figure 10: DHS

Homeland Security

Supplemental Form: Witness(es)



SAR 2.0

Witnesses: New Item

Witness Name *

Full Name of the Individual who may have witnessed the incident.

Witness Address

A number and name that identifies a particular unit or location within a street.

Witness City

Code identifying the city.

Witness State

Code identifying the state.

Witness Zip Code

The zip code or postal code.

Witness Phone Number

A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument.

Witness Phone Type

●

○ Specify your own value:

Witness Email

An electronic mailing address by which a person or organization may be contacted.

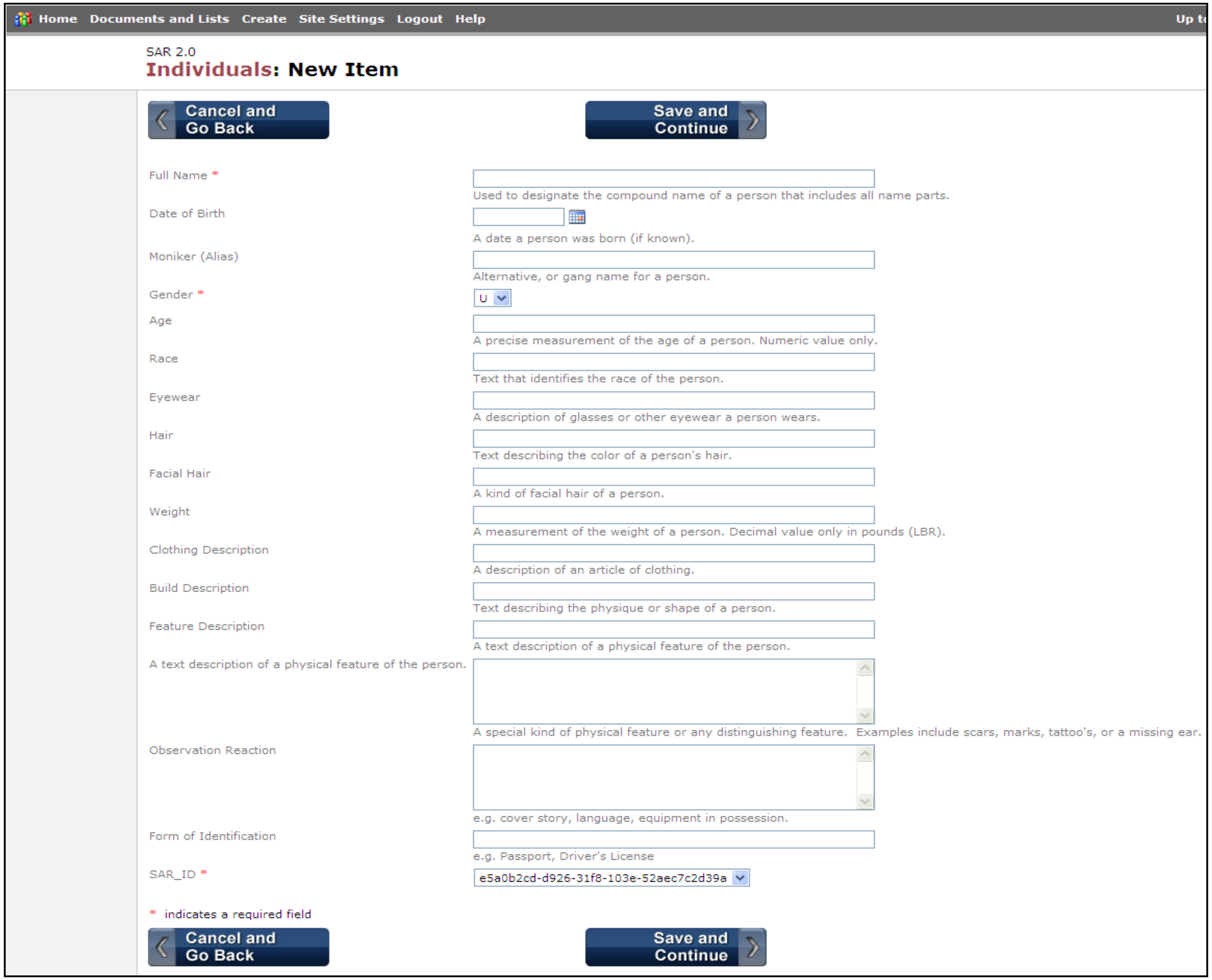
Additional Witness Information

SAR_ID * e5a0b2cd-d926-31f8-103e-52aec7c2d39a

* indicates a required field

Figure 11: DHS

Supplemental Form: Individual(s) Involved



SAR 2.0

Individuals: New Item

Full Name *
Used to designate the compound name of a person that includes all name parts.

Date of Birth
A date a person was born (if known).

Moniker (Alias)
Alternative, or gang name for a person.

Gender * U

Age
A precise measurement of the age of a person. Numeric value only.

Race
Text that identifies the race of the person.

Eyewear
A description of glasses or other eyewear a person wears.

Hair
Text describing the color of a person's hair.

Facial Hair
A kind of facial hair of a person.

Weight
A measurement of the weight of a person. Decimal value only in pounds (LBR).

Clothing Description
A description of an article of clothing.

Build Description
Text describing the physique or shape of a person.

Feature Description
A text description of a physical feature of the person.

A text description of a physical feature of the person.
A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoo's, or a missing ear.

Observation Reaction
e.g. cover story, language, equipment in possession.

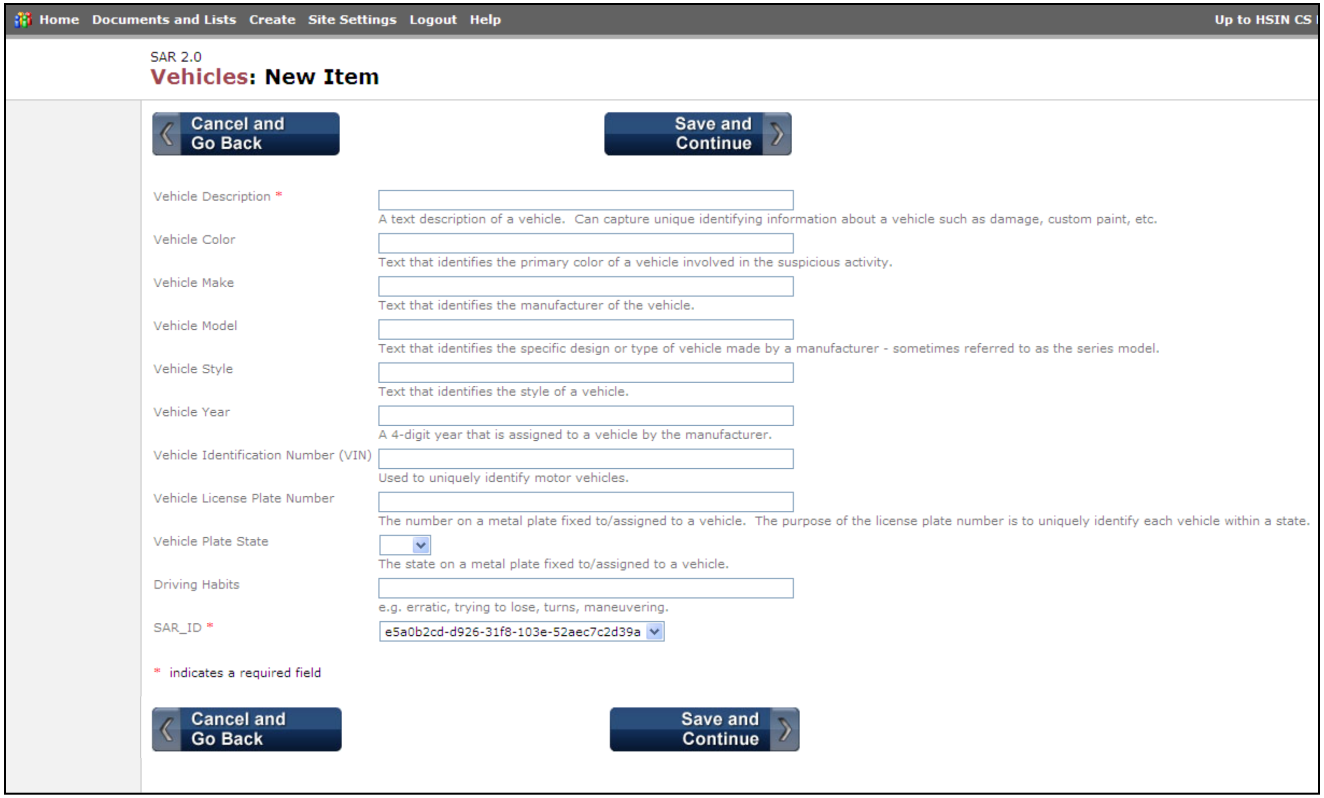
Form of Identification
e.g. Passport, Driver's License

SAR_ID * e5a0b2cd-d926-31f8-103e-52aec7c2d39a

* indicates a required field

Figure 12: DHS

Supplemental Form: Vehicle(s) Involved



SAR 2.0

Vehicles: New Item

Vehicle Description *
A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc.

Vehicle Color
Text that identifies the primary color of a vehicle involved in the suspicious activity.

Vehicle Make
Text that identifies the manufacturer of the vehicle.

Vehicle Model
Text that identifies the specific design or type of vehicle made by a manufacturer - sometimes referred to as the series model.

Vehicle Style
Text that identifies the style of a vehicle.

Vehicle Year
A 4-digit year that is assigned to a vehicle by the manufacturer.

Vehicle Identification Number (VIN)
Used to uniquely identify motor vehicles.

Vehicle License Plate Number
The number on a metal plate fixed to/assigned to a vehicle. The purpose of the license plate number is to uniquely identify each vehicle within a state.

Vehicle Plate State
The state on a metal plate fixed to/assigned to a vehicle.

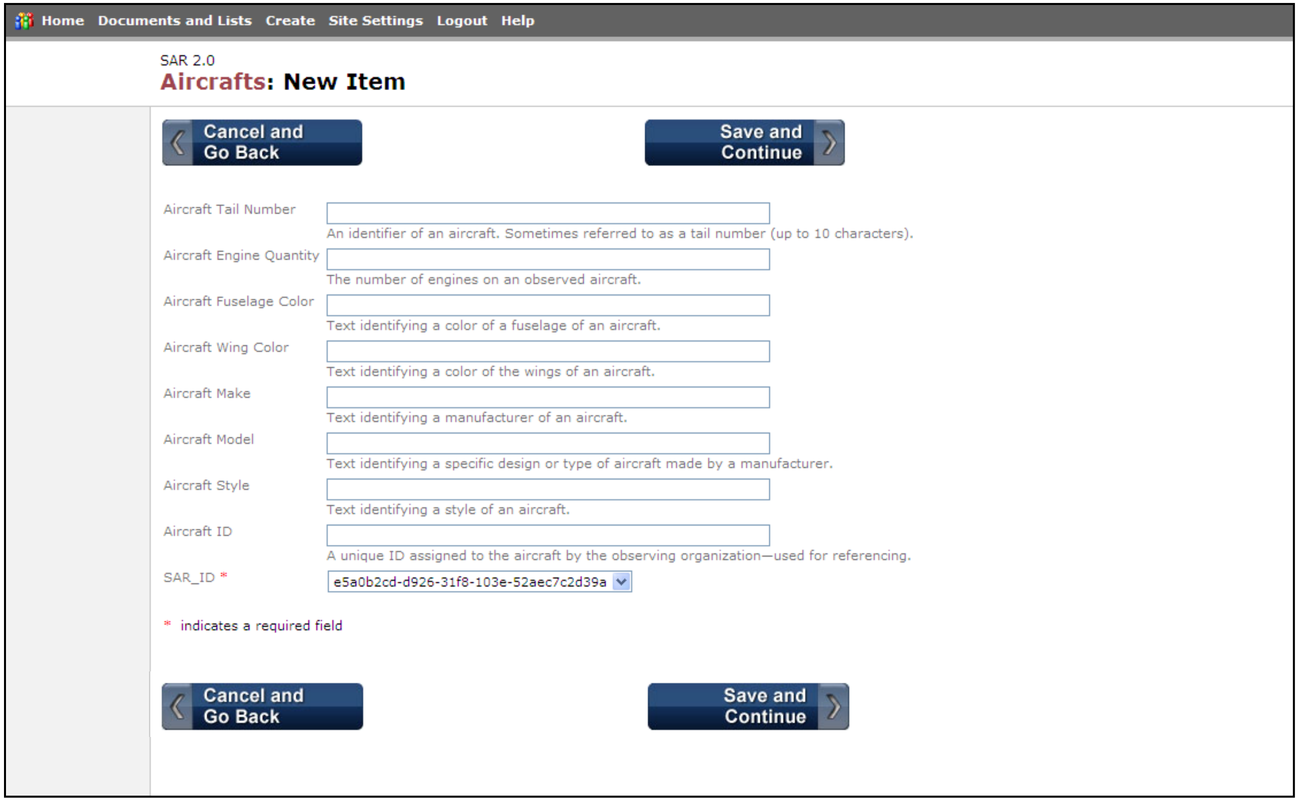
Driving Habits
e.g. erratic, trying to lose, turns, maneuvering.

SAR_ID * e5a0b2cd-d926-31f8-103e-52aec7c2d39a

* indicates a required field

Figure 13: DHS

Supplemental Form: Aircraft(s) Involved



SAR 2.0

Aircrafts: New Item

Aircraft Tail Number
An identifier of an aircraft. Sometimes referred to as a tail number (up to 10 characters).

Aircraft Engine Quantity
The number of engines on an observed aircraft.

Aircraft Fuselage Color
Text identifying a color of a fuselage of an aircraft.

Aircraft Wing Color
Text identifying a color of the wings of an aircraft.

Aircraft Make
Text identifying a manufacturer of an aircraft.

Aircraft Model
Text identifying a specific design or type of aircraft made by a manufacturer.

Aircraft Style
Text identifying a style of an aircraft.

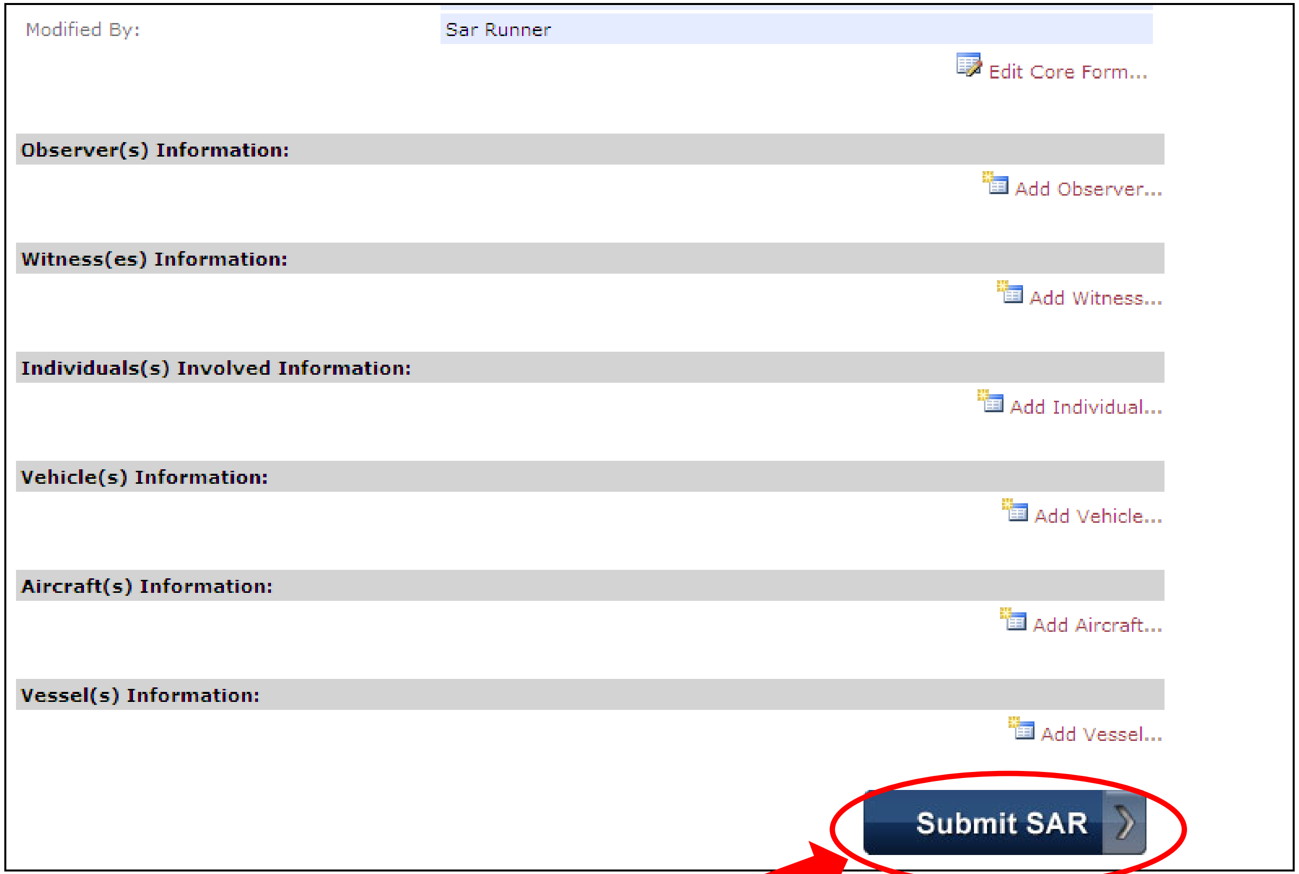
Aircraft ID
A unique ID assigned to the aircraft by the observing organization—used for referencing.

SAR_ID * e5a0b2cd-d926-31f8-103e-52aec7c2d39a

* indicates a required field

Figure 14: DHS

Submit Your SAR



Modified By: Sar Runner

Observer(s) Information:

Witness(es) Information:

Individuals(s) Involved Information:

Vehicle(s) Information:

Aircraft(s) Information:

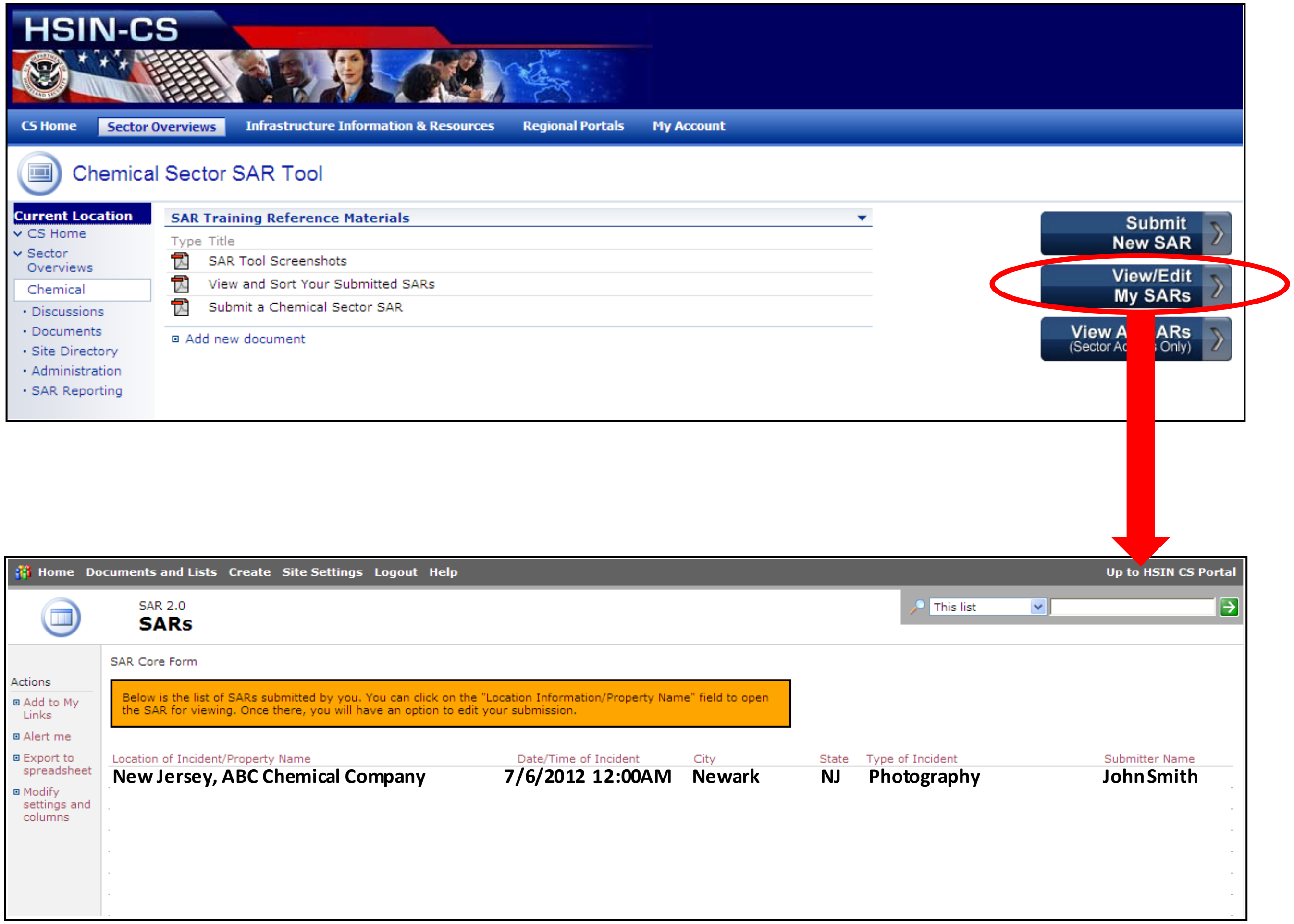
Vessel(s) Information:

Click on “Submit SAR” once
you have completed the report .

Figure 15: DHS

Homeland Security

View/Edit Your SAR



Chemical Sector SAR Tool

SAR Training Reference Materials

Type	Title
	SAR Tool Screenshots
	View and Sort Your Submitted SARs
	Submit a Chemical Sector SAR

Add new document

SAR 2.0
SARs

SAR Core Form

Below is the list of SARs submitted by you. You can click on the "Location Information/Property Name" field to open the SAR for viewing. Once there, you will have an option to edit your submission.

Location of Incident/Property Name	Date/Time of Incident	City	State	Type of Incident	Submitter Name
New Jersey, ABC Chemical Company	7/6/2012 12:00AM	Newark	NJ	Photography	John Smith

Figures 16 &17: DHS

Homeland Security

Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

Cherie Williams
HSIN-CS Implementation Manager
Sector Outreach and Programs Division
Cherylann.Williams@hq.dhs.gov