



Thomas J. Sniscak
(717) 703-0800
tjsniscak@hmslegal.com

Whitney E. Snyder
(717) 703-0807
wesnyder@hmslegal.com

100 North Tenth Street, Harrisburg, PA 17101 Phone: 717.236.1300 Fax: 717.236.4841 www.hmslegal.com

February 18, 2020

VIA ELECTRONIC FILING

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, Filing Room
Harrisburg, PA 17120

Re: Meghan Flynn, et al., Docket Nos. C-2018-3006116 & P-2018-3006117 (consolidated)
Melissa DiBernardino, Docket No. C-2018-3005025 (consolidated)
Rebecca Britton, Docket No. C-2019-3006898 (consolidated)
Laura Obenski, Docket No. C-2019-3006905 (consolidated)
Andover Homeowner's Association, Inc.; Docket No. C-2018-3003605 (consolidated)
v.
Sunoco Pipeline L.P.

**SUNOCO PIPELINE L.P. ANSWER OPPOSING FLYNN COMPLAINANTS'
MOTION TO RECLASSIFY ANSWERS TO INTERROGATORIES**

Dear Secretary Chiavetta:

Attached for electronic filing with the Commission is Sunoco Pipeline L.P.'s Answer Opposing Flynn Complainants' Motion to Reclassify Answers to Interrogatories.

If you have any questions regarding this filing, please contact the undersigned.

Very truly yours,

Thomas J. Sniscak
Whitney E. Snyder
Counsel for Sunoco Pipeline L.P.

WES/das
Enclosure

cc: Honorable Elizabeth Barnes (by email and first class mail)
Per Certificate of Service

**BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

MEGHAN FLYNN et al.	:	Docket Nos.	C-2018-3006116 (consolidated)
	:		P-2018-3006117
MELISSA DIBERNARDINO	:	Docket No.	C-2018-3005025 (consolidated)
REBECCA BRITTON	:	Docket No.	C-2019-3006898 (consolidated)
LAURA OBENSKI	:	Docket No.	C-2019-3006905 (consolidated)
ANDOVER HOMEOWNER'S ASSOCIATION, INC.	:	Docket No.	C-2018-3003605 (consolidated)
	:		
	:		
v.	:		
	:		
SUNOCO PIPELINE L.P.	:		

**SUNOCO PIPELINE L.P. ANSWER OPPOSING FLYNN COMPLAINANTS' MOTION
TO RECLASSIFY ANSWERS TO INTERROGATORIES**

Pursuant to 52 Pa. Code § 5.61, Sunoco Pipeline L.P. (SPLP) files this Answer Opposing Flynn Complainants' January 28, 2020 Motion to Reclassify Answer to Interrogatories (Motion). SPLP is not required to admit or deny allegations of the Motion,¹ particularly given it is unverified. Failure to deny any allegation shall not be deemed an admission.

In Section I, SPLP proves that the information Complainants seek to reclassify is appropriately designated as Confidential Security Information, Highly Confidential. In Section II, SPLP provides a paragraph by paragraph response to the Motion. This Answer is verified by Matthew Gordon, Senior Director of Liquid Pipeline Operations for SPLP.

¹ Compare 52 Pa. Code § 5.61(b)-(c) (allegations in complaint may be deemed admitted if not specifically denied) with 52 Pa. Code § 5.103 (regarding response to motions and containing no similar provision).

I. THE INFORMATION AT ISSUE IS CONFIDENTIAL SECURITY INFORMATION, HIGHLY CONFIDENTIAL

1. By their motion to reclassify highly confidential security information, the Flynn Complainants, who call themselves the “Safety Seven,” actually attempt to jeopardize public safety by seeking to release to the public information that terrorists or other bad actors could use to cause public harm. This is not just SPLP’s opinion regarding this type of information, but it is one the Legislature, this Commission,² the U.S. Department of Homeland Security, the U.S. Congress, and the Governmental Accountability Office all hold.

2. Flynn Complainants dispute SPLP’s designation of Interrogatory Response 44(l) as Highly Confidential, Confidential Security Information pursuant to the Amended Protective Order and the Public Utility Confidential Security Information Disclosure Protection Act (CSI Act). Interrogatory Response 44(l) provides a detailed and specific timeline of events taken in response to a release of gasoline near the Tunbridge Apartment complex on Monday, November 11, 2019.

3. When Flynn Complainants contacted SPLP regarding this designation, SPLP responded that it would create another public version of the Response to 44(l). This version only redacts the detailed and specific times of SPLP’s initial awareness of the event, response and arrival to the scene, and emergency responders’ timing of arrival to the scene, as well as the staging area that the emergency responders used. A copy of this public version of the response to 44(l) is included as **Attachment A**.

4. Thus, the only information that requires designation as Highly Confidential, Confidential Security Information (the information at issue here) is specific timing between SPLP’s initial awareness of the event, the time it took SPLP to respond and arrive to the scene, the

² The Commission adopted regulations to protect such information.

timing of emergency responders arrival to the scene, and the precise location where emergency responders set up their staging area.

5. This information is properly designated as Confidential Security Information and thus as Highly Confidential pursuant to the Amended Protective Order.³ Detailed and specific timing from an actual event (time of awareness of the event through times when SPLP and emergency responders took action and arrived to the scene of the event) and where emergency responders located during the event is information that the CSI Act protects because this information could “compromise security against sabotage or criminal or terrorist acts” and the “nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities.” CSI Act at Section 2 (defining CSI). The Federal Government recognizes the security sensitive nature of this type of information in that it can be used to maximize success and impact of a potential attack and the importance of protecting pipeline-related security sensitive information. *Infra* ¶¶ 9-13.

6. In short, the information is required to be protected from public disclosure as Highly Confidential CSI because the release of pipeline incident response time information and location of emergency responders would provide terrorists or other bad actors with the knowledge necessary to: interfere with the pipeline operator’s and emergency responders’ actions in response to a pipeline emergency; and/or or conduct secondary attacks on or diversions of emergency responders and pipeline operator personnel, thus increasing the potential for significant loss of life and/or damage to property. Specific details on when and how the pipeline operator and/or

³ Amended Protective Order at ¶ 4 (“Moreover, information subject to protection under the Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and PUC Regulations at 52 Pa. Code §§ 102.1-102.4 will also be designated as ‘HIGHLY CONFIDENTIAL PROTECTED MATERIAL’ . . .”).

emergency responders respond to a pipeline incident would allow a person with ill intent to plan and more successfully execute unlawful actions based on when and how emergency responders and pipeline operator personnel respond to an actual pipeline incident.

7. The CSI Act defines confidential security information in relevant part as:

Information contained within a record maintained by an agency in any form, **the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities, including, but not limited to**, all of the following:

(1) A vulnerability assessment which is submitted to the Environmental Protection Agency or any other Federal, State or local agency.

(2) Portions of emergency response plans that are submitted to the Department of Environmental Protection, the Pennsylvania Public Utility Commission or any other Federal, State or local agency **dealing with response procedures** or plans prepared to prevent or respond to emergency situations, except those portions intended for public disclosure, **the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures or specific security procedures**. Nothing in this term shall be construed to relieve a public utility from its public notification obligations under other applicable Federal and State laws.

(3) A plan, map or other drawing or data which shows the location or reveals location data on community drinking water wells and surface water intakes.

(4) A security plan, security procedure or risk assessment prepared specifically for the purpose of preventing or for protection against sabotage or criminal or terrorist acts.

(5) (i) Specific information, including portions of financial statements, about security devices or personnel, designed to protect against sabotage or criminal or terrorist acts. (ii) Nothing in this definition shall be construed to prevent the disclosure of monetary amounts.

CSI Act at Section 2 (emphasis added).

8. The CSI Act unquestionably protects incident response time frames and procedures. While the information at issue is not contained specifically in one of the documents

listed in the definition of CSI, the Act is clear that the list is non-exclusive. *Id.* (Information... **the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities, including, but not limited to**) (emphasis added). Moreover, time frames and procedures to respond to an event are the specific type of information that could be contained in an emergency response plan pursuant to subsection 2 that the Act specifically protects. *Id.* (“Portions of emergency response plans ... **dealing with response procedures** or plans prepared to prevent or respond to emergency situations, except those portions intended for public disclosure, **the disclosure of which would reveal** vulnerability assessments, **specific tactics, specific emergency procedures or specific security procedures.**”) (emphasis added).

9. The U.S. Department of Homeland Security issued a report that shows how incident response time frames and procedures could be used to endanger the public, emergency responders, and pipeline operator personnel. U.S. Dep’t of Homeland Security, Planning Considerations: Complex Coordinated Terrorist Attacks (July 2018) (“DHS CCTA Report”). The DHS CCTA Report is included as **Attachment B**. The DHS CCTA Report explains tactics terrorists or others may use, based on prior attacks, to maximize harm from a potential attack:

[b]ased on assessments of previous CCTAs, attackers may employ the following tactics, techniques, and procedures:

- **Use pre-attack surveillance and reconnaissance to gather intelligence for tactical planning and execution;**

...

- **Strike multiple targets simultaneously or in close succession;**
- **Strike quickly and move to another location before law enforcement can interdict and disrupt;**
- **Deploy diversions to slow public safety response, consume responder resources, or draw/reorient responders toward or away from specific locations;**

...

- Coordinate attack timing and methods (e.g., firearms, IEDs, Hazardous Materials [HazMat]) with other attackers and parties providing assistance to assault teams;
- **Conduct secondary attacks on first responders, evacuation routes, and/or additional sites, such as medical facilities, that are part of the response;**
- **Adapt and adjust tactics and/or location quickly based on law enforcement and first responder actions;**

Id. (emphasis added).

10. Based on this report and if the information at issue was publicly disclosed, a terrorist could find it in pre-attack reconnaissance, and then knowing specific and actual response times of SPLP and emergency responders and the specific location of emergency responders' staging area, use that information to know how long they have and where: to attack one location before moving to the next; initiate an attack against emergency responders; wait at the scene to divert or attack responders; and/or otherwise adapt and adjust their tactics or location based on these time frames and location information.

11. A person seeking to maximize harm from his intentional attack on the pipeline would find great value in knowing when and how to disrupt plans for responding to that attack. Thus, specific incident response timing and location could aid attackers in targeting multiple attack locations, "further compound[ing] the complexity of the incident," DHS CCTA Report at 5, and potentially aid in "disrupting essential functions, services, and capabilities across the whole community," *id.* at 7, where "[t]he different attack locations and potential for follow-on attacks may cause confusion among responders and hamper attempts to gather and disseminate accurate information in real time." *Id.* at 4. Release of emergency response times would aid attackers in drawing out first responders and pipeline operator personnel to increase the potential of maximum destruction or in creating diversion of resources to commit other attacks.

12. The DHS CCTA Report discussion of tactics terrorists may use proves that the information redacted here (timing of response and location of emergency responders during an incident) would be of value to a terrorist or other bad actor deploying these tactics and maximizing their effectiveness. Thus, this information is confidential security information because it could “compromise security against sabotage or criminal or terrorist acts” and the “nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities.” CSI Act at Section 2 (defining CSI).

13. Moreover, the policy behind protection of information that could aid bad actors in harming the public, emergency responders, and pipeline operator personnel mandates a broad application of the Act. A March 2019 U.S. Congressional Research Report summarizes threats faced by pipelines and the importance of ensuring the security of pipeline infrastructure, explaining:

Ongoing threats against the nation’s natural gas, oil, and refined product pipelines have heightened concerns about the security risks to these pipelines, their linkage to the electric power sector, and federal programs to protect them. In a December 2018 study, the Government Accountability Office (GAO) stated that, since the terrorist attacks of September 11, 2001, “new threats to the nation’s pipeline systems have evolved to include sabotage by environmental activists and cyber attack or intrusion by nations.” In a 2018 Federal Register notice, the Transportation Security Administration stated that it expects pipeline companies will report approximately 32 “security incidents” annually—both physical and cyber.

...

Congress and federal agencies have raised concerns since at least 2010 about the physical security of energy pipelines, especially cross-border oil pipelines. These security concerns were heightened in 2016 after environmentalists in the United States disrupted five pipelines transporting oil from Canada. In 2018, the Transportation Security Administration’s Surface Security Plan identified improvised explosive devices as key risks to energy pipelines, which “are vulnerable to terrorist attacks largely due to their stationary nature, the volatility of transported products, and [their] dispersed nature.” Among these risks, according to some analysts, are the

possibility of multiple, coordinated attacks with explosives on the natural gas pipeline system, which potentially could “create unprecedented challenges for restoring gas flows.”

Paul Parfomak, Cong. Research Serv., IN11060, *Pipeline Security: Homeland Security Issues in the 116th Congress* (2019). Further explaining pipelines vulnerability to outside attacks, the Government Accountability Office (GAO)’s December 2018 study on pipeline security found:

According to TSA, pipelines are vulnerable to physical attacks—including the use of firearms or explosives—largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. The nature of the transported commodity and the potential effect of an attack on national security, commerce, and public health make some pipelines and their assets more attractive targets for attack. Oil and gas pipelines have been and continue to be targeted by terrorists and other malicious groups globally.⁴

II. RESPONSES TO NUMBERED PARAGRAPHS OF THE MOTION

1. Admitted.

2. Admitted.

3. Complainants’ past allegations are irrelevant to the Motion at issue. Regardless of what Complainants alleged in their prior motion, SPLP denied those allegations and that motion was deemed withdrawn. January 2, 2020 Order Admitting Stipulation Into the Record at Ordering ¶ 4 (“Complainants’ Motion to Reclassify Putative Confidential Documents filed on November 8, 2019, is deemed withdrawn.”).

4. Admitted in part, denied as stated in part. Interrogatory 44 was a 12-part interrogatory consisting of requests (a)-(l). Admitted that request 44(l) is accurately represented

⁴ U.S. Gov’t Accountability Off., GAO-19-48, *Critical Infrastructure Protection Actions Needed to Address Significant Weaknesses in TSA’s Pipeline Security Program Management*, pgs. 10-11 (Dec. 2018), available at <https://www.gao.gov/assets/700/696123.pdf>.

in the Motion. To clarify, the only portion of SPLP's response that SPLP designated as Highly Confidential, Confidential Security Information and Complainants' place at issue in their Motion is the Response to 44(l).

5. Denied. SPLP did not redact the entirety of its response to Interrogatory 44 as Flynn Complainants misrepresent. SPLP includes as **Attachment C** its response to the entirety of Interrogatory 44. SPLP only redacted the response to 44(l) in the initial public version of its response as Highly Confidential, Confidential Security Information. Denied to the extent implied that SPLP did not provide an unredacted response to 44(l) to appropriate and authorized counsel pursuant to the Amended Protective Order, including Flynn Complainants' counsel. In fact, counsel for the Flynn Complainants has obtained an unredacted version of SPLP's response to 44(l), which he can use subject to the terms of the Amended Protective Order, the Commission's regulations, and the Procedural Orders in this proceeding.

6. Denied to the extent it is implied that SPLP did not timely serve its response containing Highly Confidential, Confidential Security Information. Both the public and Highly Confidential, Confidential Security Information versions of the response were timely served on January 13, 2020.

7. The purpose of discovery is for a party to prepare for litigation of a case: "(f) *Purpose and methods*. A party may obtain discovery for the purpose of preparation of pleadings, or for preparation or trial of a case, or for use at a proceeding initiated by petition or motion, or for any combination of these purposes." 52 Pa. Code § 5.321(f). The purpose of discovery is not to obtain information to disclose to the public, particularly of the Highly Confidential, Confidential Security Information contained in the response to 44(l). SPLP will not

respond to the rest of the unverified allegations in this paragraph, which are irrelevant to the disposition of this motion and not properly before Your Honor.

8. Admitted.

9. Denied. These allegations are specious and without support, particularly given that the Motion is unverified.

10. Admitted.

11. Admitted. However, Flynn Complainants fail to mention that they refused SPLP's provision of a public copy of the response to 44(l) that only redacted the times of SPLP's initial awareness of the event, response and arrival to the scene and emergency responders timing of arrival to the scene as well as the staging area emergency responders used. A copy of this version of the response to 44(l) is included as **Attachment A**.

12. Denied that Paragraph 8 of the Amended Protective Order is applicable here. Paragraph 8 is only applicable to Extremely Sensitive Materials (ESM). SPLP did not classify its response to 44(l) as ESM, but as Highly Confidential, Confidential Security Information.

13. Denied that Paragraph 8 of the Amended Protective Order is applicable here. Paragraph 8 is only applicable to ESM. SPLP did not classify its response to 44(l) as ESM, but as Highly Confidential, Confidential Security Information.

14. Denied. The response to 44(l) was not designated as ESM, but as Highly Confidential, Confidential Security Information. The redacted materials in response to 44(l) reflected in **Attachment A** are confidential security information under the Public Utility Confidential Security Information Disclosure Protection Act. *See Supra* Section I, which is incorporated herein as if set forth in full.

15. Denied as stated. SPLP has the burden under the Amended Protective Order to show that its designation is appropriate.

16. Denied as stated. The Amended Protective Order already places the burden upon SPLP to show that its designation is appropriate. It is doing so through this verified Answer. SPLP does not believe that any additional process is required given the scope of the Motion's request for reclassification.

III. CONCLUSION

WHEREFORE, SPLP respectfully requests that Flynn Complainants Motion to Reclassify Answers to Interrogatories be denied.

Respectfully submitted,



Thomas J. Sniscak, Esq. (PA ID No. 33891)
Whitney E. Snyder, Esq. (PA ID No. 316625)
Hawke, McKeon & Sniscak LLP
100 North Tenth Street
Harrisburg, PA 17101
Tel: (717) 236-1300
tjsniscak@hmslegal.com
kjmckeon@hmslegal.com
wesnyder@hmslegal.com

/s/ Robert D. Fox

Robert D. Fox, Esq. (PA ID No. 44322)
Neil S. Witkes, Esq. (PA ID No. 37653)
Diana A. Silva, Esq. (PA ID No. 311083)
MANKO, GOLD, KATCHER & FOX, LLP
401 City Avenue, Suite 901
Bala Cynwyd, PA 19004
Tel: (484) 430-5700
rfox@mankogold.com
nwickes@mankogold.com
dsilva@mankogold.com
Attorneys for Respondent Sunoco Pipeline L.P.

Dated: February 18, 2020

Attachment A

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- (k) For each person identified in response to (h) above, set forth the extent of that person's health effects and the treatment that person received.

RESPONSE: N/A

DATE: January 13, 2020

BY: Matthew Gordon

- (l) Set forth a detailed timeline of the entire release event, for each event, including but not limited to time the release commenced, when Sunoco became aware of it, how Sunoco became aware of it, when Sunoco personnel were dispatched to the scene, when Sunoco personnel arrived at the scene, the time when Sunoco first spoke with Delaware County Emergency Services, when Delaware County first responders first arrived, when the release was contained.

RESPONSE:

- The console 14 Pipeline Controller (PC) received an LEL alarm at [REDACTED] and that alarm cleared on its own (no continuous LEL reading) at [REDACTED], another LEL alarm activated at [REDACTED] and cleared on its own at [REDACTED].
- SPLP dispatched technicians to the scene at [REDACTED].
- Lead Pipeline Controller notified Technical Supervisor at [REDACTED] about the LEL alarms at Glenn Riddle Junction.
- Pipeline Operations Supervisor notified console 14 at [REDACTED] to shut down the Twin Oaks to Fullerton pipeline due odor reports from the public.
- At [REDACTED] the pipeline was shut down. PC turned off the originating pump station (Twin Oaks) and the Glenn Riddle Junction site was isolated by closing [REDACTED].
- At approximately [REDACTED] SPLP mechanic arrived on site. Various other SPLP personnel and contractors arrived on site throughout the event.
- At approximately [REDACTED], first responders arrived at [REDACTED].

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- The Company believes unknown parties contacted 911, the Fire Department and made a PEMA notification concurrently with the notification noted above. The company is not able to access / confirm this information.
- At 5:24 PM ET a Right of Way agent received a call from residents.
- At 5:27 PM ET a Right of Way agent calls resident back to let them know someone is on route to the scene.
- By 6:10 PM ET SPLP confirmed the leak was secure.
- At 6:10 PM ET, SPLP spoke with emergency responders at the scene, notified them that leak was secure and hot zone established with PID readings.
- At 6:40 PM ET, SPLP began checking homeowner properties closest to the release site and walked down the pipeline ROW in the direction of the wind with
- At 6:40 PM ET Right of Way agent speaks with another home owner.
- By 7:00 PM ET SPLP conducted gas monitoring downwind of the site and found no detectable vapors.
- At 7:07 PM ET SPLP conducted an area gas test at Glenn Riddle Junction and found no LEL detectable vapor, and PID levels less than 100 PPM.
- At 7:12 PM ET, SPLP opened the site for access.
- At 7:18 PM ET SPLP walked down the site with a gas meter for further assessment with spill response contractor.
- At 7:20 PM ET Right of Way agent spoke with the manager of the Turnbridge Apartments.
- At 7:25 PM ET SPLP updated emergency responders of gas test results and location SPLP team.
- At 7:30 PM ET site recovery begins.
- At 8:05 PM ET air monitoring via portable gas detection units to monitor air for flammable vapors were set up.

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- At 8:30 PM ET Right of Way agent met with resident to visit his home. SPLP relocated this resident at his request. SPLP went back the next morning to check on odor levels.

DATE: January 13, 2020

BY: Matthew Gordon

Attachment B



Planning Considerations: Complex Coordinated Terrorist Attacks

July 2018



Homeland
Security

Table of Contents

Complex Coordinated Terrorist Attacks: Threat Background and Characteristics	1
Purpose	1
Background	1
CCTA Characteristics	2
CCTA Challenges	3
CCTAs: Planning Considerations	8
The Six-Step Planning Process	8
Step 1: Form a Collaborative Planning Team	8
Step 2: Understand the Situation	10
Step 3: Determine Goals and Objectives	11
Step 4: Plan Development	12
Step 5: Plan Preparation, Review, and Approval	12
Step 6: Plan Implementation and Maintenance	12
Planning Checklist	14
Purpose, Scope, Situation Overview, and Planning Assumptions	14
Concept of Operations	14
Direction, Control, and Coordination	15
Communications	15
Administration, Finance, and Logistics	16
Preparedness, Mitigation, and Recovery	16
Implementation, Maintenance, and Training	16
Authorities and References	16
CCTAs: Risk Assessment Considerations	17
Step 1: Identify the Threats and Hazards of Concern	17
Step 2: Give the Threats and Hazards Context and Estimate Impacts	17
Potential Consequences	17
Examples of CCTA Context Description	18
Estimated Impacts	19
Step 3: Establish Capability Targets	20
CCTAs: Resources	21
Training Resources	21
Technical Assistance Resources	21
Resource Types	23
Other Resources	23

This page intentionally left blank.

Complex Coordinated Terrorist Attacks: Threat Background and Characteristics

Complex Coordinated Terrorist Attacks (CCTAs)

CCTAs are acts of terrorism that involve synchronized and independent team(s) at multiple locations, sequentially or in close succession, initiated with little or no warning, and employing one or more weapon systems: firearms, explosives, fire as a weapon, and other nontraditional attack methodologies that are intended to result in large numbers of casualties.

Purpose

This guide supports planning for Complex Coordinated Terrorist Attacks (CCTAs) and provides a summary of their unique characteristics. The document builds on *Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans*, and *CPG 201: Threat and Hazard Identification and Risk Assessment (THIRA) Guide* by providing planning considerations specific to CCTAs, which are relevant both to developing a plan and to completing a THIRA.

Background

CCTAs are an evolving and dynamic terrorist threat, shifting from symbolic, highly planned attacks to attacks that could occur anywhere, at any time, with the potential for mass casualties and infrastructure damage. Although some characteristics of a CCTA are similar to an active shooter incident (e.g., use of firearms, potential for large numbers of fatalities, responding organizations and resources), the complexities of CCTAs (e.g., multiple teams, attack locations, and weapon types) may represent additional challenges to jurisdictions. CCTAs require the delivery of community capabilities and resources across a wide range of Core Capabilities.¹ Table 1 lists examples of real-world CCTAs.

¹ For more information on Core Capabilities, visit: <https://www.fema.gov/core-capabilities>.

Table 1: CCTA Examples

CCTA Incident	Method	Consequence
Madrid, 2004	Train Bombings	1,800+ Wounded, 190 Killed
London, 2005	Train and Bus Bombings	784 Wounded, 52 Killed
Mumbai, 2008	Firearms, Bombings, and Arson	308 Wounded, 164 Killed
Paris, 2015	Firearms and Bombings	368 Wounded, 130 Killed
Brussels, 2016	Airport and Train Bombings	330 Wounded, 32 Killed
Alexandria/Tanta, 2017	Church Bombings	126 Wounded, 45 Killed
Barcelona, 2017	Vehicle Ramming and Knife Attack	130 Wounded, 16 Killed

These incidents demonstrate how attackers can assemble trained teams, acquire explosives, weapons, and communications equipment, exploit open-source information to gather intelligence on targets, and successfully carry out acts of extreme violence. Over time, assailants study and learn from each other, improving their tactics to counter first responders and law enforcement in an effort to increase casualties, inflict maximum damage at attack sites, and prolong incidents to achieve sustained media coverage. Targeted acts of violence that have no direct connection to terrorism may employ tactics that mimic CCTAs and would require the same level of coordination to be managed effectively.

CCTA Characteristics

Based on assessments of previous CCTAs, attackers may employ the following tactics, techniques, and procedures:

- Use pre-attack surveillance and reconnaissance to gather intelligence for tactical planning and execution;
- Use small teams of well-armed, well-trained individuals employing military or law enforcement style tactics;
- Select soft targets or other vulnerable environments to maximize casualties;
- Strike multiple targets simultaneously or in close succession;
- Strike quickly and move to another location before law enforcement can interdict and disrupt;
- Employ assault weapons, explosives, improvised explosive devices (IEDs), and/or fire as weapons; may use/incorporate other nontraditional methods, such as vehicle ramming, knifing attacks, and dispersing chemical or biological agents.
- Delay or deny exit by victims and entry by public safety by blocking exits and/or chaining/rigging doors with explosives, using tear gas, and/or using fire/smoke to delay law enforcement response efforts and potentially prolong the incident;
- Take hostages to prolong the incident and/or delay law enforcement response efforts;

- Deploy diversions to slow public safety response, consume responder resources, or draw/reorient responders toward or away from specific locations;
- Exploit social media and news coverage to maximize shock value, spread misinformation, instill fear, and promote extreme views;
- Communicate effectively across assault teams, targets, and with outside leadership;
- Coordinate attack timing and methods (e.g., firearms, IEDs, Hazardous Materials [HazMat]) with other attackers and parties providing assistance to assault teams;
- Conduct secondary attacks on first responders, evacuation routes, and/or additional sites, such as medical facilities, that are part of the response;
- Adapt and adjust tactics and/or location quickly based on law enforcement and first responder actions; and
- Learn from past law enforcement and first responder tactics and prior CCTA incidents.

CCTA Challenges

Based on the CCTA threat, jurisdictions may face the following specific challenges when addressing CCTAs:

- **Operational Coordination.** The complexity of these attacks requires responders to counter with a fully integrated and coordinated response. The ability to respond to, and subsequently recover from, a CCTA will involve personnel and resources from a range of disciplines such as fire, law enforcement, emergency management, emergency medical services, healthcare, and transportation. Some of these contributors may come from the private sector. A major challenge of a CCTA incident is integrating crisis management (e.g., law enforcement, interdiction), consequence management (e.g., emergency management), and investigatory functions (e.g., evidence gathering, forensics, attribution), which must be performed simultaneously and involve entities that may not habitually operate together. To address the dispersed geographical nature of a CCTA and the likely diversity of responding entities, jurisdictions should plan, prepare for, and be proficient in unified command/area command. The ability to rapidly assemble and/or recall and deploy additional resources to multiple locations is vital. Planning should include considerations for sustained operations across multiple operational periods for all responding public safety and support staff. Based on historic events, operations may include both day and night operations.

A CCTA consists of a number of small teams whose intent is to overwhelm a jurisdiction's capabilities by targeting multiple geographically dispersed locations and maximizing fatalities through attack methods and denial of access to casualties. While "on duty" law enforcement may have enough resources and experience to stop attackers at one location, jurisdictions may face challenges addressing attacks and coordinating the response at multiple locations. CCTA tactics may involve attackers breaking contact with law enforcement and moving to a new target or escaping before being contained at the initial attack site. Similarly, the strategy of maximizing fatalities by denying access to casualties could overwhelm emergency medical response capabilities and resources. Determining the necessary resources and planning for access to those resources (i.e., mutual aid agreements) is key to an effective CCTA response. CCTAs also can occur across jurisdictional

boundaries, underscoring the importance of maintaining situational awareness, pre-incident planning, and coordination among regional partners to respond and implement CCTA plans when an initial incident presents evidence of complexity or coordination of attackers at multiple locations.

- **Incident Command.** A well-coordinated incident command system is critical for an effective response to a CCTA. The different attack locations and potential for follow-on attacks may cause confusion among responders and hamper attempts to gather and disseminate accurate information in real time. A cohesive approach to incident command ensures that command officers from impacted entities (e.g., law enforcement, fire, emergency medical services (EMS), public health, public works) have accurate information and can help accomplish unified incident objectives. The National Incident Management System (NIMS) describes the systems, principles, and structures that provide a standard, national framework for incident management.² Under NIMS, the Incident Commander is the individual responsible for on-scene incident activities. Selection of an Incident Commander is based a range of factors including qualifications, experience, type of incident, and location, not rank or title.

The complex nature of a CCTA (e.g., multiple attackers, multiple locations, multidisciplined response) may require a quick transition from a single Incident Commander to a Unified Command to coordinate a joint response from multiple agencies. A Unified Command enables organizations from multiple disciplines to have a voice in determining common priorities and supports the safe synchronization of personnel and resources.

- **Area Command/Unified Area Command.** The existence of multiple, complex attack sites may require the establishment of an Area Command. The Area Command:
 - Provides management and coordination for two or more incidents in close proximity;
 - Establishes shared objectives and maintains a shared common operating picture during the CCTA; and
 - Works directly with the individual Incident Commanders to prioritize and allocate resources.

An Area Command may be located at an Emergency Operations Center (EOC) facility or at another location different from the Incident Command Post (ICP) to avoid confusion with the ICP activities.

An Area Command becomes a Unified Area Command once the incident becomes multijurisdictional. The Unified Area Command serves the same role as an Area Command, with representatives from impacted jurisdictions comprising the command staff. Under both Area Command and Unified Area Command, the tactical and operational responsibilities for incident management activities reside with the individual on-scene Incident Commander. Coordinated planning, training, and exercises among organizations, disciplines, and jurisdictions potentially affected by a CCTA should address likely command structures, activation triggers, staffing, and communication protocols.

² Federal Emergency Management Agency, *National Incident Management System*, (Washington, DC) <https://www.fema.gov/national-incident-management-system>. See ICS Tab 7—Consolidating the Management of Multiple Incidents.

- **Operational Communication.** CCTAs may occur with little to no warning. Establishing timely communications among and between the affected communities, and all responding disciplines, is critical to an effective response. An effective communication infrastructure within the affected areas supports security operations and enhances the allocation of incident response resources to the right location at the right time. Incident response plans should incorporate a multidisciplinary communications approach to address emerging life-saving and life-sustaining operations. Mobile radios with assigned interagency channels, WebEOC, geospatial information systems, mapping programs, and other communication capabilities can enhance situational awareness and create and maintain a common operation picture. Jurisdictions should regularly test and exercise operational communication plans and mechanisms.
- **Public Information and Warning.** During a CCTA, promptly disseminating accurate crisis information and guidance to the public is essential for stabilizing the situation and, potentially, for saving lives. Crisis information may include instructions for the public related to protective actions to avoid the effects of a CCTA (e.g., shelter-in-place), or to avoid specific areas or infrastructure (e.g., public transit). Local, state, tribal, and federal systems such as the Integrated Public Alert and Warning System (IPAWS) and the Emergency Alert System facilitate communication with the public, including individuals with access and functional needs. IPAWS allows authorized alerting authorities to send a single message through multiple communication platforms and devices to reach as many people as possible to save lives and protect property.

A Joint Information System (JIS) provides a coordinated joint approach among response partners to deliver accurate crisis information during and after incidents, including a CCTA. Implementing a JIS, and identifying a Joint Information Center (JIC) where public information activities are coordinated can help ensure timely, accurate, accessible, consistent, and unified messaging across multiple stakeholders; minimize confusion; and quickly dispel rumors and disinformation. Jurisdictions should consider developing and exercising prepackaged crisis information messaging that is adaptable in the event of a CCTA. Prepackaged messaging may include alerts, warnings, or notifications (e.g., shelter-in-place, lockdown, evacuation activations). Both the messages and the mechanisms for distributing those messages should account for the demographics and resources of the jurisdiction to ensure accurate and accessible information reaches the whole community.

Jurisdictions should consider including relevant media outlets in pre-event coordination to determine public information procedures and protocols during a CCTA. Involving the media as planning partners can reduce the dissemination of inaccurate or sensitive information that could endanger the public, degrade the incident response, or interfere with the incident investigation. In addition to traditional media outlets, planners should consider using social media to rapidly distribute accurate public information and messages. By monitoring social media, responding agencies and incident managers can quickly identify and counter erroneous information and rumors and increase situational awareness.

- **Multiple Attack Locations.** One characteristic of a CCTA is the occurrence of incidents at multiple locations sequentially or in quick succession. Identifying a second attack at an additional location signifies that the incident has expanded from a single-site incident (e.g., active shooter, arson) to a CCTA. Subsequent attacks further compound the complexity of

the incident. Planning efforts should reflect that attack sites will transition toward recovery individually, based on the status of response operations at each location.

- **Initial Attack:** When the initial (only known) attack is identified or occurs, jurisdictions respond, rapidly establish an incident command, and mobilize, deploy, and/or employ appropriate capabilities to counter or lessen the impacts of the incident. Initial response efforts focus on stopping and/or containing the threat, preventing loss of life through life-saving and life-sustaining actions, and issuing immediate public safety messages and press release statements.
- **Subsequent Attack(s):** As a subsequent attack(s) occurs or is identified, responding agencies gain situational awareness, establish ingress/egress routes, activate coordination centers, reallocate deployed resources, alert or deploy follow-on resources, and request local, state, and/or Federal assistance. Jurisdictions may also begin investigative and intelligence operations.
- **Recovery:** Recovery efforts begin during incident response and may occur simultaneous to law enforcement and first responder activities, depending on the security and safety at the individual attack locations. Recovery activities may include providing continued medical (including behavioral health) response, conducting family reunification efforts, conducting follow-on investigative and intelligence operations, and initiating whole community recovery and mitigation actions.
- **Self-Deployment/Self-Dispatch.** FEMA, state, and local authorities highly discourage first responders and other emergency personnel from self-dispatching, but some individuals nonetheless self-dispatch. Authorities should direct self-dispatched responders back to their home organization, which may work with local incident managers to determine if and how additional responders may integrate into the response. Self-deploying can cause safety risks to responders, civilians, and others who are operating within the perimeters of the incident. It can also create additional risks, such as blocked emergency ingress/egress routes, delay of responders gaining access to the site, loss of personnel accountability, and slowing transport of critically injured personnel from the scene.
- **Rescue Task Force (RTF).** The dangers associated with CCTA incidents, like active shooter incidents, may limit the ability of emergency medical service personnel to attend to victims in a timely manner. An RTF combines law enforcement with fire/EMS personnel to bring medical support into “warm zones” of the incident scene where some risk exists, but has been minimized by the law enforcement response. RTFs allow faster victim stabilization and evacuation from the scene, but require collaboration, planning and advanced training among law enforcement and fire/EMS personnel.
- **Healthcare.** A CCTA may result in mass casualties. Hospitals near the scene of an attack will likely receive an influx of walk-in wounded survivors in addition to those patients transported by EMS. The large number of casualties will drive a need for pre-hospital care, triage, emergency workers’ personal protection equipment (PPE), and patient accountability capabilities. Healthcare facilities may implement preplanned protective actions for their facility, which could slow the patient care or patient transfer from EMS. Mass casualty events could potentially overwhelm healthcare resources and cause coordination difficulties (e.g., limited space or staff available to support initial casualties; require patient redistribution; influx of non-triaged casualties into emergency care facilities). Jurisdictions

should establish procedures to provide situational awareness and keep incident commanders informed of any hospitals and other medical facilities overwhelmed by patients, to include self-transported individuals. Hospital personnel, with EOC support, may need to coordinate ambulances and transportation support to relocate patients from hospitals and medical facilities that receive but cannot manage large numbers of patients. A CCTA requires an organized response by all elements of the healthcare system, including first responders, transportation providers, decontamination teams, and all levels of clinical care facilities. Time, coordination, and communication among all of these elements is essential.

- **Fatality Management Services.** A CCTA may overwhelm available resources to address the timely and respectful recovery, identification, processing, and release of fatalities. Planning efforts should include subject matter experts, such as representatives from coroner or medical examiner offices; mortuary service providers; or Disaster Mortuary Operational Response Team personnel, if local, to consider aspects of fatality management. Example functions include collecting, documenting, transporting, storing, and identifying fatalities and next of kin notification, and providing behavioral health assistance to survivors. Jurisdictions may consider establishing a family assistance or identification center. A CCTA, as a terrorist or criminal act, requires coordination among law enforcement and coroners/medical examiners regarding evidentiary considerations and requirements.
- **Bystander/Survivor Response.** Planners need to consider the role of bystanders following a CCTA. In many instances, these individuals are the initial First Care Providers until emergency response personnel arrive. The lifesaving actions and initiative of bystanders and survivors can benefit response efforts. Examples of actions that individuals take when faced with a CCTA include immediate lifesaving medical support, providing comfort to the injured, implementing lockdown procedures, and assisting in transporting individuals from the scene. National programs and initiatives such as “Tactical Emergency Casualty Care” (TECC),³ “Stop the Bleed,”⁴ and “You Are the Help Until Help Arrives”⁵ provide individuals the critical knowledge and training to take simple, potentially lifesaving steps should the need arise. These measures may be key to mitigating casualties in the interval between the time of an attack and the point when emergency medical responders arrive on the scene. Planners should also consider that bystanders and survivors might serve as valuable witnesses and support incident investigation efforts.
- **Continuity of Operations.** CCTAs may occur at any time and at multiple locations, disrupting essential functions, services, and capabilities across the whole community. Organizations, both government and private sector, located in and near the affected areas may experience disruptions of routine operations and/or loss of infrastructure or critical systems. Effective continuity planning and operations increase resiliency and ensure that organizations can continue to provide essential functions and services during an incident. FEMA’s *Continuity Guidance Circular* provides detailed guidance on continuity planning and operations.⁶

³ For more information on TECC, visit <https://c-tecc.org>.

⁴ For more information on “Stop the Bleed,” visit dhs.gov/stopthebleed.

⁵ For more information on “You Are the Help Until Help Arrives,” visit <https://community.fema.gov/until-help-arrives>.

⁶ FEMA, *Continuity Guidance Circular*, (Washington, DC, 2018), <https://www.fema.gov/continuity-guidance-circular-cgc>.

CCTAs: Planning Considerations

Planning efforts must integrate the whole community across the Prevention, Protection, Mitigation, Response, and Recovery mission areas. The focus on whole community inclusion, combined with a capability-based approach, helps planners enhance preparedness for all threats and hazards, including CCTAs. This guidance focuses on developing and maintaining a CCTA incident annex, which describes roles and responsibilities, integration mechanisms, and actions required of a jurisdiction and its partners as a result of, and in response to, a CCTA. Communities must develop plans based on likely requirements and the capabilities necessary to meet those requirements. Planners should review and revise these plans as the planning process continues and capabilities change.

The Six-Step Planning Process

Figure 1 shows the six step planning process described in *Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans*⁷. While CPG 101 explains the individual steps in detail, the discussion below focuses on planning considerations related to the development or revision of a CCTA incident annex.

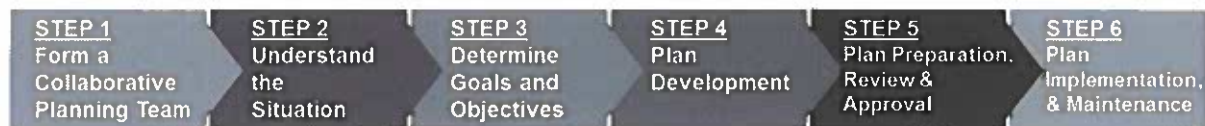


Figure 1: Six-Step Planning Process

Step 1: Form a Collaborative Planning Team

The most realistic and complete plans result from a diverse planning team that includes representatives from the organizations that have roles in the coordination, delivery, execution, and support of capabilities necessary to address a CCTA. Example stakeholders may come from the following organizations/entities:

Law Enforcement

- Local, state, tribal, or territorial law enforcement
- Federal Bureau of Investigation (FBI)
- Law enforcement intelligence units
- Joint Terrorism Task Force
- Special Weapons and Tactics (SWAT)
- Fusion centers

- Bomb Squads.

Fire Service/Medical Services

- Fire service
- Emergency medical services (EMS)
- Hospitals and healthcare facilities
- Mental health
- Medical assistance teams
- Medical examiner.

⁷ FEMA, *CPG 101: Developing and Maintaining Emergency Operations Plans, Version 2.0*, (Washington, DC, 2010), <https://www.fema.gov/media-library/assets/documents/25975>.

Public Safety

- Local, state, tribal, territorial, and regional emergency management
- 911 call center/dispatch/communication center
- Public health
- Public works
- Transportation (e.g., public transportation systems, local transportation departments)
- Emergency Operations Center (EOC)
- National Guard
- Hazardous materials units
- Public safety communications.

Education

- School administration
- Academia (e.g., expert researchers, facilitators)
- School resource officers.

Other Governments and Agencies

- Tribal governments
- State governmental agencies (e.g., procurement, legal, traffic engineering, housing and urban development)
- Local governmental agencies (e.g., procurement, legal, traffic engineering, housing and urban development)
- Public information/External affairs
- Disability services

- Social Services
- Federal departments/agencies
- Elected officials
- Coast Guard.

Private Sector

- Chambers of commerce
- Critical infrastructure owners and operators (public and private)
- Cellular communication providers
- Retail entities (e.g., small businesses, utilities, big-box stores, shopping malls)
- Media outlets (including social media)
- Educational and professional organizations
- Security organizations
- Union officials.

Nongovernmental Organizations

- American Red Cross
- Volunteer organizations
- Civic organizations
- Social organizations
- Faith-based organizations
- Advocacy organizations (e.g., organizations that address disability and access and functional needs issues, children's issues, immigrant and racial/ethnic community concerns, animal welfare, service animals).

Core Planning Team

The core planning team, a subset of the larger collaborative planning team, should be a small group of staff that will write the plan. Many jurisdictions have personnel with law enforcement, fire service, public health, EMS, or other special emergency planning expertise. Their expertise can strengthen the core planning team and inform the development, implementation, and refinement of the CCTA incident annex. For a CCTA incident annex,

Table 2 shows a potential initial core planning team, their roles in addressing CCTA response and recovery planning, and example organizations.

Table 2: Example Core Planning Team Members

Planning Team Member	Role	Example Organizations
Law Enforcement	<p>Leads prevention, protection, and collaborative mitigation strategies and primary response</p> <p>Leads investigations, apprehending suspects, rendering potential threats safe</p> <p>Part of RTF component</p>	Police and sheriff's departments
Emergency Management	<p>The lead planning coordinator</p> <p>Provides expertise on jurisdiction's emergency plans, activities, and resources along with guidance on CCTA preparedness planning in collaboration with Law Enforcement.</p>	Local emergency management agencies
Fire Service	<p>Leads the suppression and containment of fire and HazMat incidents</p> <p>Part of RTF component</p>	Fire departments
Emergency Medical Services	<p>Leads the operational medical care and transportation of victims</p> <p>Part of RTF component</p>	Ambulance/emergency medical services
Hospitals	<p>Coordinate primary medical care and lifesaving efforts in partnership with operational medical units</p>	Hospitals, healthcare, and behavioral health facilitates
Public Health	<p>Leads the identification of and dissemination of information about threats to public health and mitigation efforts.</p>	Health departments

Step 2: Understand the Situation

Prior to developing a CCTA incident annex, planners should understand their Emergency Operations Plan (EOP) and any existing supporting plans. This is important because annexes supplement the EOP; a CCTA incident annex therefore should be consistent with the EOP and not duplicate or conflict with it. A jurisdiction's base EOP or supporting plans will address many of the responsibilities and actions taken during a CCTA, as they are frequently required regardless of the specific threat or hazard. A CCTA incident annex should address the unique characteristics and requirements associated with a CCTA incident (e.g., incident-specific concept of operations, roles, responsibilities).

Once assembled, the planning team begins identifying potential consequences and impacts of a CCTA on the community and the capabilities necessary to address those consequences. The CCTAs: Risk Assessment Considerations section of this document provides information and guidance on understanding the potential consequences of a CCTA and potential CCTA scenarios. Communities that complete the Threat and Hazard Identification and Risk Assessment (THIRA)⁸ process should use existing THIRA analysis to guide their efforts during this step. Jurisdictions also should use existing plans and resources such as capability assessments and after-action reviews to inform their planning efforts. CPG 101 provides additional detail on conducting research and analysis on potential threats and hazards and assessing associated risk.

Step 3: Determine Goals and Objectives

In Step 3, the planning team identifies operational priorities and develops a list of goals and objectives relative to a CCTA. These goals and objectives help inform the development of potential courses of action in the subsequent step. Sample goals and objectives for a CCTA might include:

- **Goal 1: Stop/contain the threat to prevent further loss of life.**
 - Objective 1.1: Deploy law enforcement team(s) to stop/contain threat utilizing tactical deployment based on the situation.
 - Objective 1.2: Deploy fire/HazMat team(s) to detect, contain, and remove any release or potential release of hazardous substances to control or stabilize the incident.
 - Objective 1.3: Establish and secure ingress/egress routes.
 - Objective 1.4: Establish Incident Command.
 - Objective 1.5: Alert or deploy follow-on resources.
 - Objective 1.6: Coordinate with the EOC/Joint Operations Center.
 - Objective 1.7: Conduct render-safe activities, if needed.
 - Objective 1.8: Identify and respond to subsequent attack.
 - Objective 1.9: Establish a Unified Area Command, if required by response.
 - Objective 1.10: Establish regular communications with the fusion center.
 - Objective 1.11: Gain and maintain situational awareness at additional sites.
- **Goal 2: Provide timely life-saving and life-sustaining actions to those in need, from the point of wounding onward.**
 - Objective 2.1: Deploy multidisciplinary teams to provide necessary medical care at the point of injury (e.g., RTF).
 - Objective 2.2: Evacuate casualties to critical care facilities.
 - Objective 2.3: Coordinate with hospitals and care facilities to determine their ability to receive mass casualties.
 - Objective 2.4: Provide medical assistance at additional attack sites.

⁸ Federal Emergency Management Agency, *CPG 201: Threat and Hazard Identification and Risk Assessment Guide, Third Edition*, (Washington, DC), [fema.gov/threat-and-hazard-identification-and-risk-assessment](https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment).

- Goal 3: Create and maintain public messaging.
 - Objective 3.1: Establish a JIC.
 - Objective 3.2: Disseminate alert messaging through JIC/EOC.
 - Objective 3.3: Issue protective action guidance to public.
- Goal 4: Secure potential high-priority target sites.
 - Objective 4.1: Assess the risk and location of potential future sites.
 - Objective 4.2: Coordinate security operations at additional at-risk sites based on the initial attack profile.
 - Objective 4.3: Activate mutual aid agreements, request resources to facilitate protective measures at additional sites.
- Goal 5: Initiate recovery and post-incident activities.
 - Objective 5.1: Establish operational reunification/survivor assistance centers.
 - Objective 5.2: Conduct ongoing intelligence/investigations operations.
 - Objective 5.3: Re-establish compromised critical infrastructure in the affected area, if necessary.

Step 4: Plan Development

Based on the priorities, goals, and objectives from Step 3, the planning team begins developing the plan. Planners can develop multiple courses of action to answer the “what, who, when, where, why, how” questions to satisfy Step 3’s objectives and actions. After developing courses of action, planners compare the costs and benefits of each proposed course of action against the goals and objectives. Based on this comparison, planners select preferred course(s) of action to move forward with resource identification and additional informational requirements. The selected course(s) of action should consider resource allocation and prioritization efforts likely required by a CCTA (e.g., prevention vs. response, multiple attack sites/scenes). Planners should refer to CPG 101 for detailed guidance on developing, analyzing, and selecting courses of action.⁹

Step 5: Plan Preparation, Review, and Approval

Once the team develops a plan, representatives from the organizations involved in the CCTA response should review it to validate the existing content and potentially identify additional coordination points, functions, or resources. After this broader review, the appropriate senior officials receive the plan for final review, approval, and signature, publication, and dissemination.

Step 6: Plan Implementation and Maintenance

Jurisdictions should implement the plan through training and exercises so stakeholders throughout the whole community know their roles and responsibilities before, during, and after a CCTA incident. All organizations named in the plan and supporting partners should train to, exercise, and become familiar with the plan. Successful implementation of the plan includes

⁹ FEMA, *CPG 101: Developing and Maintaining Emergency Operations Plans, Version 2.0*, (Washington, DC, 2010), <https://www.fema.gov/media-library/assets/documents/25975>.

training personnel and organizations to deliver the capabilities, functions, and procedures that the plan requires of them. Through exercises, incident managers further their practical understanding of their partner organizations' procedures and capabilities. Exercises also help to address any known gaps, identify potential resource shortfalls or weakness in the plan, and serve as an opportunity to identify lessons learned. The knowledge resulting from both training activities and exercises, along with real-world events and the identification of new resources are vital considerations for the ongoing review and future revision of the CCTA plan.

Planning Checklist

The following checklist provides considerations for producing, reviewing, and updating a CCTA plan or annex.

Purpose, Scope, Situation Overview, and Planning Assumptions

- **Purpose**
 - ☐ Indicate the reason the annex exists
 - ☐ Include a statement of what the annex is meant to achieve
- **Scope**
 - ☐ List trigger points for annex implementation
 - ☐ Clearly indicate when the CCTA annex is no longer applicable and operations are complete
- **Situation Overview**
 - ☐ Describe the characteristics of a CCTA, including the specific threats, hazards, and risks associated with a CCTA
 - ☐ Define what constitutes a CCTA
 - ☐ Incorporate capabilities and capacity from all identified planning partners
 - ☐ Include additional contact and location information pertaining to partner capabilities
- **Planning Assumptions**
 - ☐ Contain a list of planning assumptions specific to the CCTA incident

Concept of Operations

- ☐ Describe likely command structures and requirements associated with a CCTA incident
- ☐ Identify the lead organization for specific functions within a CCTA scenario
- ☐ Indicate who has authority to declare a state of emergency
- ☐ Explain that operational phases may be different for each attack scene and how coordination should happen in those instances
- ☐ Indicate that actions at individual incident scenes may vary based on attack characteristics and circumstances at each location
- ☐ Address sustained operations for all responding and support staff
- ☐ Describe the process for allocating resources to multiple scenes
- ☐ Identify operational priorities (e.g., prevention of additional attacks versus immediate response)
- ☐ Describe the process for identifying prevention and response activities and deploying resources
- ☐ Address how to prioritize and execute enhanced security operations at potential high-risk attack sites based on the assessment of the initial attack profile

- ☐ Address how hospitals near the scene of an attack will receive a large influx of walk-in patients, in addition to transported patients
- ☐ Address pre-hospital care, triage, emergency worker self-protection, and patient accountability
- ☐ Address how to establish and operate a family assistance/identification center
- **Organizing and Assigning Responsibilities**
 - ☐ Incorporate appropriate whole community partner agencies and organizations
 - ☐ List responsible agencies and partners and their assigned roles and responsibilities
- **Mutual Aid**
 - ☐ Identify anticipated mutual aid partners in event of a CCTA
 - ☐ Indicate the necessary resources and mechanisms to activate them (e.g., mutual aid agreements)
 - ☐ Describe any prerequisites for requesting mutual aid resources
 - ☐ Identify communication and coordination mechanisms between mutual aid resources and Unified Command

Direction, Control, and Coordination

- ☐ Identify organizations represented in a Unified Coordination Group
- ☐ Provide a clear unity of command when involving multiple organizations and multiple incident scenes
- ☐ Address how Incident Command will address large geographic distances between scenes

Communications

- **Operational Communication**
 - ☐ Identify a mechanism to ensure timely, accurate, and consistent messaging across disciplines and jurisdictions (e.g., JIS)
 - ☐ Identify support organizations, capabilities, and teams to establish an effective and continuous interoperable communication, including cellular communications
- **Public Information and Warning**
 - ☐ Establish a JIC to facilitate the flow of critical emergency information, crisis communications, and public affairs communications
 - ☐ Provide a coordinated joint approach among response partners to deliver crisis information during and after a CCTA to ensure timely, accurate, accessible, and consistent messaging across multiple stakeholders, to minimize confusion and dispel rumors
 - ☐ Address messaging and distribution mechanisms to account for the demographics and resources of the jurisdiction
 - ☐ Address the use of social media to distribute public information rapidly to prevent inaccurate or misleading information

Administration, Finance, and Logistics

- ☐ Identify administrative controls used to provide resource and expenditure accountability

Preparedness, Mitigation, and Recovery

- ☐ Incorporate short-term, intermediate, and long-term recovery strategies/objectives
- ☐ Address how to implement support plans for survivors and families of the deceased
- ☐ Include strategies to implement the Recovery Support Functions (RSFs) after the incident
- ☐ Include how to provide mental health assistance and support in recovery support efforts
- ☐ Outline remediation procedures for damaged or hazardous sites

Implementation, Maintenance, and Training

- ☐ Identify applicable, available CCTA training
- ☐ Identify exercise program requirements and timelines
- ☐ Identify/summarize how and to whom the plan is distributed; indicate whether it is shared with the public
- ☐ Include a schedule to review and revise the plan
- ☐ Identify the process used to review and revise the plan
- ☐ Include all partners involved in the annex development in the maintenance of the plan and training schedule
- ☐ Outline the responsibility of partners to review and provide changes to the plan; identify the process to provide feedback

Authorities and References

- ☐ Include a list of the relevant authorities
- ☐ Include links to applicable references and guidance

CCTAs: Risk Assessment Considerations

Communities use the THIRA¹⁰ process to identify the capabilities required to address anticipated and unanticipated risks. FEMA encourages jurisdictions to involve the whole community in the THIRA process. Private, public, and nonprofit sector stakeholders and subject matter experts can share information, identify community-specific considerations, and help communities better understand the initial and cascading effects of a particular threat or hazard.

Step 1: Identify the Threats and Hazards of Concern

In Step 1 of the THIRA, communities develop a list of threats and hazards. To be included in the assessment, each threat or hazard must meet two criteria: (1) it must have the realistic potential to affect the community and (2) it must challenge at least one of the Core Capabilities more than any other threat or hazard. The number of threats and hazards that each community may face depends on the individual community's risk profile.

Step 2: Give the Threats and Hazards Context and Estimate Impacts

In Step 2 of the THIRA, communities add descriptions for each of the threats and hazards they have selected, describing a scenario that shows how the threat or hazard may affect the community and create challenges in performing the Core Capabilities. Scenarios include critical details such as location, magnitude, and time of an incident.

Communities also estimate the impacts these scenarios would have on their community if they occurred. If an element of the scenario is essential to understanding the impact of an incident and the capabilities required to manage it, the community should include that element in the context description. The Complex Coordinated Terrorist Attacks: Threat Background and Characteristics section of this document provides key characteristics of CCTAs.

Potential Consequences

Understanding the potential consequences of CCTAs will help planners identify and estimate capability requirements and potential impacts, which is essential to effective planning. CCTAs could occur in any jurisdiction, at any time, with the potential for mass casualties and infrastructure damage. Table 3 provides additional details on the scenarios and impacts of the CCTAs identified in Table 1.

¹⁰ For more information on the THIRA process, see CPG 201 at <https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment>.

Table 3: Consequences of CCTAs

CCTA Incident	Consequences
Madrid, Spain (2004)	13 members of an Al Qaeda-affiliated network placed 13 backpacks and bags, each containing an estimated 10 kg of explosives and metal fragments, on four different trains bound for Madrid, Spain. Ten of the bombs detonated, nearly simultaneously, resulting in more than 1,800 injuries and 190 deaths.
London, England (2005)	Four Islamist extremists set off suicide bombs targeting London's transit system. The attack left 52 people dead (not including the four suicide bombers), with 784 injured.
Mumbai, India (2008)	Lashkar-e-Taiba, an Islamic militant organization based in Pakistan, carried out a series of 12 coordinated shooting and bombing attacks lasting four days across Mumbai, India. The attacks killed 164 people and wounded at least 308 others.
Paris, France (2015)	Over the course of three hours, suicide-bomber gunmen killed 130 people and injured 368 others in attacks on six different locations, including a series of restaurants and a concert venue.
Brussels, Belgium (2016)	Suicide bombers detonated three explosive devices, two at Zaventem International Airport and one at the Maelbeek Metro Station. The blasts killed 32 people and injured more than 330.
Alexandria/Tanta, Egypt (2017)	Two suicide bombers detonated explosive devices at churches on Palm Sunday, killing 45 individuals and injuring more than 120.
Barcelona/Cambriis, Spain (2017)	Attackers drove vehicles into crowds of pedestrians, and then stabbed bystanders with knives while attempting to escape. The attacks killed 16 people and injured more than 130 others. Authorities believe the assailants resorted to vehicle ramming after explosives planned for use in their attacks accidentally exploded.

Examples of CCTA Context Description

Context descriptions transform a generic threat or hazard into a scenario. Context descriptions include critical details that affect the size of the impacts to the jurisdiction and their capabilities, including time, location, magnitude, and other community resilience factors that might affect the extent of an event's impacts.

CCTA Scenario 1

During a busy Saturday in a metropolitan area, a terror cell executes a coordinated attack. Several cell members deploy to local parks, outdoor markets, and other mass gatherings with pressure-cooker IEDs and automatic weapons. The intent is to detonate the IEDs and use their automatic weapons to cause additional casualties. At 12:00 p.m., the devices detonate and the gunmen open fire on survivors as well as first responders. At that same moment, three other small groups of the same terror cell attack pre-identified targets, including a shopping center, a hotel, and a popular entertainment district that includes multiple, large restaurants. Using IEDs, grenades, fire, and automatic weapons, these three locations are now under siege. Explosions occur at the shopping center and entertainment district while incendiaries ignite in the hotel, causing fires throughout the building. Law enforcement has responded, but due to limited resources, it is difficult to ascertain the number of assailants at any one location. After 90

minutes of explosions and gun battles across the metro area, the attacks result in 85 casualties, 323 injuries of various degrees of severity, and a large-scale psychological impact on the community. Law enforcement believes they have stopped/contained all threats, but remain on high alert for follow-on attacks.

CCTA Scenario 2

During a heavy rush hour commute on a Friday evening in a major metropolitan area, a group of terrorists launches a complex coordinated attack against the city's transit system. Beginning at 5:30 p.m., numerous IEDs and suicide vests detonate on buses and subway cars, as well as vehicle-borne IEDs (VBIEDs) underneath rail bridges. As responders arrive and passengers evacuate to several subway stations, other terrorists embedded in the crowd detonate remote IED devices on platforms, and use automatic weapons to cause additional fatalities and take hostages. In total, four subway stations have now become hostage situations, each with approximately 40 hostages. The terrorists use social media to claim responsibility, promise follow-on attacks, and broadcast the hostage executions. After several hours, law enforcement is able to free all remaining hostages and stop 16 terrorists. Authorities count 130 casualties and 425 injuries, and the city government assesses extensive damage to its public transportation system from structural damage to tunnels, trains, and buses. The city government also expects a large psychological impact on its residents, affecting ridership on the system. Law enforcement remains on high alert for follow-on attacks, particularly due to conflicting reports by witnesses and hostages of the number of suspects.

Estimated Impacts

In addition to developing context descriptions, communities estimate the impacts that each scenario would have on their jurisdictions if the threat or hazard occurred. The THIRA process uses a uniform set of common emergency management metrics, referred to as standardized impact language. The standardized impact language represents metrics estimated by every community and in most cases, across multiple different threats and hazards. Table 4 lists examples of impacts selected for a CCTA (Note: this is an abridged list, only displaying standard impacts relevant to a CCTA).

Table 4: Example CCTA Impacts

Standard Impact Language	Impact Number
(#) people requiring medical care	78
(#) people affected	210
(#) people with access and functional needs affected	32
(#) fatalities	12
(#) structure fires	9
(#) jurisdictions affected	3
(#) partner organizations involved in incident management	12
(#) HazMat release sites	1

Step 3: Establish Capability Targets

In THIRA Step 3, communities establish capability targets, which define success for each Core Capability and describe what the jurisdiction wants to achieve. Communities use standardized language provided by FEMA, but identify community-specific metrics to complete these targets. In addition to the required capability targets, communities may also develop additional targets. Table 5 includes example standard targets applicable to CCTAs.

Table 5: Example CCTA Standard Capability Targets

Mission Area	Core Capability	Capability Target
Response	On-scene Security, Protection, and Law Enforcement	Within (#) (time) of an incident, provide security and law enforcement services to protect emergency responders and (#) people affected.
Response	Fatality Management Services	Within (#) (time) of an incident, complete recovery, identification, and mortuary services, including temporary storage services, for (#) fatalities.
Response	Public Health, Healthcare, and EMS	Within (#) (time) of an incident, complete triage, begin definitive medical treatment, and transfer to an appropriate facility (#) individuals requiring medical care.
Response	Situational Assessment	Within (#) (time) of incident, and on a (#) (time) cycle thereafter, notify leadership and (#) partner organizations involved in incident management of the current and projected situation. Maintain for (#) (time).
Cross-Cutting	Operational Coordination	Within (#) (time) of a potential or actual incident, establish and maintain a unified and coordinated operational structure and process across (#) jurisdictions affected and with (#) partner organizations involved in incident management. Maintain for (#) (time).

CCTAs: Resources

Training Resources

- **FEMA National Training and Education Division (NTED):** Provides training to the emergency management community, other homeland security professionals, and our citizens to enhance their skills for preventing, protecting, responding to, and recovering from manmade and natural catastrophic events. The following CCTA related training courses can be found at firstrespondertraining.gov/:
 - Situation Assessment for Complex Attacks (PER-328-W)
 - Critical Decision Making for Complex Coordinated Attacks (PER-335)
 - Active Shooter Incident Management with Complex Incidents (PER-353)
 - Advance Tactical Operations WMD Interdiction (PER-277)
 - Initial Law Enforcement Response to Suicide Bombing Attacks (PER-232)
 - Introduction to Tactical Emergency Casualty Care for First Care Providers (PER-356)
- **FEMA Emergency Management Institute (EMI).** EMI serves as the emergency management community's flagship training institution and provides training to local, state, tribal, territorial, Federal, volunteer, public, and private sector officials to strengthen emergency management core competencies for professional, career-long training. The following CCTA-related training courses are available at training.fema.gov/emi/:
 - E912: Preparing Communities for a Complex Coordinated Attack
 - Incident Command System (ICS) 400: Advanced Incident Command System for Command and General Staff – Complex Incidents
- **Center for Domestic Preparedness.** The Center for Domestic Preparedness provides advanced, all-hazards training emergency responders from state, local, tribal, and territorial governments, as well as the Federal government, foreign governments, and private entities. The scope of training includes preparedness, protection, and response.
 - Hospital Emergency Response Training for Mass Casualty Incidents (HERT PER-902)
- **Federal Law Enforcement Training Centers (FLETC).** FLETC is the nation's largest provider of law enforcement training. A component of the Department of Homeland Security (DHS), FLETC provides basic and advanced training annually to local, state, tribal, territorial, Federal, and international law enforcement organizations. Information on available course is located at <https://www.fletc.gov/>. Relevant CCTA offerings include:
 - Law Enforcement First Responder Training Program
 - Tactical Medical for First Responders course

Technical Assistance Resources

- **Joint Counterterrorism Awareness Workshop Series (JCTAWS):** JCTAWS is a two-day workshop comprised of briefings and facilitated discussions in breakout groups. Participants separate into four functional breakout groups: Senior Command, Operations, Community

Coordination, and Medical Coordination. A team of local and Federal facilitators lead each breakout group. They guide discussions and assist participants in identifying successful practices and gaps in planning, coordination, and current operational capabilities. Each breakout group maintains a slightly different focus, based on the everyday roles and responsibilities of the participants. Additionally, each breakout group is cross-populated with representatives from the other breakout groups to promote a more comprehensive discussion. At the conclusion of the breakout sessions, each breakout group reports back to the larger group and captures these findings for the Summary Report.

For more information, contact FEMA National Exercise Division at NEP@fema.dhs.gov.

- **Complex Coordinated Terrorist Attack Technical Assistance (C2TA) Program:** C2TA is a gap analysis and planning workshop series specifically designed for communities that receive Federal funding to support planning, training, and exercising for a CCTA. C2TA is designed for core planners of primary public safety and emergency response organizations, including law enforcement, intelligence, dispatch/communications, fire service, emergency medical service, emergency management, and critical public infrastructure partners. C2TA brings together planners from different disciplines and agencies to define the gaps in their regional plans for a CCTA and to refine those gaps into actionable steps to improve their plans, training, and exercise programs. As a result of attending C2TA, jurisdictions will:
 - Define gaps in current operational capabilities for a CCTA
 - Organize gaps to support ongoing efforts in planning, training, and exercising for a CCTA
 - Recognize the vulnerabilities of interdependent emergency response and critical infrastructure systems in a CCTA
 - Improve cooperation between and across agencies and jurisdictions.
- **National Exercise Program (NEP):** The NEP is the principal mechanism for examining and validating core capabilities nationwide across all mission areas (Prevention, Protection, Mitigation, Response, and Recovery). The NEP consists of a two-year, progressive cycle of select exercises across the homeland security enterprise anchored to a common set of strategic objectives—called Principals’ Objectives—that culminates in a biennial National Level Exercise. Exercises are nominated into the NEP and selected based on their alignment to the Principals’ Objectives. The types of exercises selected into the program may include facilitated policy discussions, seminars and workshops, tabletop exercises, drills, functional exercises, and full-scale exercises—all of which may be sponsored by organizations from any level of government, non-governmental and private sector organizations, and other partners across the whole community. For more information or to nominate an exercise into the NEP, contact the FEMA National Exercise Division at NEP@fema.dhs.gov.

Resource Types

The following are example resources from FEMA's NIMS Resource Typing Library Tool (RTLTL),¹¹ which may be applicable in a CCTA response. Jurisdictions should include other resources that address their specific needs for a successful response.

- Air Ambulance (Rotary-Wing)
- Air Medical Transport Paramedic
- Air Medical Transport Manager
- Ambulance
- Ambulance Strike Team
- Bomb Squad/Explosive Team
- Behavioral Health Community Services Team
- Behavioral Health Specialist
- Critical Incident Stress Management Team
- Disaster Collapsed Structure Canine Search Technician
- Emergency Medical Responder
- Emergency Medical Task Force
- Emergency/Critical Care Team
- Emergency Medical Physician
- Engine, Fire (Pumper)
- Fatality Management Disaster Portable Morgue Unit
- Fire Truck – Aerial (Ladder or Platform)
- Law Enforcement Strike Team
- Law Enforcement Helicopter (Patrol)
- Mass Casualty Support Vehicle
- Medical Search and Rescue Technician
- Mobile Communications Unit
- Mobile Communications Center (Mobile EOC)
- Paramedic
- Public Information Officer
- Social Worker
- Strike Team, Engine (Fire)
- Structural Collapse Rescue Team
- SWAT/Tactical Teams
- Urban Search and Rescue Task Force

Other Resources

- **First Responder Guide for Improving Survivability in Improvised Explosive Device and/or Active Shooter Incidents:** This Federal multidisciplinary first responder guidance translates evidence-based response strategies from the U.S. military's vast experience in responding to and managing casualties from IED and/or active shooter incidents. Evidence-based strategies also come from its significant investment in applying combat casualty care research to the civilian first responder environment. Additionally, the guidance incorporates civilian best practices and lessons learned from similar incidents, both in the United States and abroad.

Recommendations developed in this paper fall into three general categories: hemorrhage control, protective equipment (which includes, but is not limited to, ballistic vests, helmets, and eyewear), and response and incident management.

[dhs.gov/sites/default/files/publications/First Responder Guidance June 2015 FINAL 2.pdf](https://dhs.gov/sites/default/files/publications/First%20Responder%20Guidance%20June%202015%20FINAL%202.pdf)

¹¹ For more information on the RTLTL, visit <https://rtltoolkit.fema.gov/Public>.

- **Improving Active Shooter/Hostile Event Response: Best Practices and Recommendations for Integrating Law Enforcement, Fire, and EMS:** This report informs communities of the value and necessity of developing an integrated response to future active shooter/hostile events (ASHEs), with the long-term goal of influencing change in first responder ASHE response. The findings of this report center around two objectives: (1) share ASHE lessons learned from participating municipalities and agencies and identify similarities and differences in response plans, and (2) develop specific recommendations for integrating law enforcement, fire, and EMS response.
[interagencyboard.org/sites/default/files/publications/External IAB Active Shooter Summit Report.pdf](https://interagencyboard.org/sites/default/files/publications/External%20IAB%20Active%20Shooter%20Summit%20Report.pdf)
- **Training Trigger: Integrated Response Operations in Active Shooter/Hostile Events (ASHE):** This fact sheet provides a brief overview of ASHE operational issues, fast facts, activities, templates/best practices, and other resources.
[interagencyboard.org/sites/default/files/publications/Training Trigger - Integrated Response Operations in ASHE.pdf](https://interagencyboard.org/sites/default/files/publications/Training%20Trigger%20-%20Integrated%20Response%20Operations%20in%20ASHE.pdf)
- **Continuity Guidance Circular:** The Circular details the fundamental theories and concepts to unify the application of continuity principles, planning, and programs across the Nation. Continuity of operation ensures that the whole community has essential services to function when disruptions to normal operations occur. It provides the importance of incorporating the specific risks into continuity planning for awareness, preparedness, planning, and coordination between Federal and non-Federal entities. <https://www.fema.gov/media-library/assets/documents/132130>
- **Core Capability Development Sheets:** FEMA's Core Capability Development Sheets identify tools for organizations to sustain or improve their capabilities to close identified gaps. <https://www.fema.gov/core-capability-development-sheets>
- **You Are the Help Until Help Arrives:** A nationwide campaign to empower individuals to act quickly to provide first care in the aftermath of an incident. This campaign focuses on five essential actions, including moving someone away from ongoing danger, stopping life-threatening bleeding, positioning the injured so they can breathe, keeping them warm, and providing comfort. <https://community.fema.gov/until-help-arrives>
- **Stop the Bleed:** A nationwide campaign to empower individuals to act quickly and save lives. It provides resources to help the public learn more about bleeding control and how to act in a situation that requires immediate responders. dhs.gov/stopthebleed
- **Integrated Public Alert and Warning System (IPAWS):** IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System, Wireless Emergency Alerts, the National Oceanic and Atmospheric Administration Weather Radio, and other public alerting systems from a single interface. <https://www.fema.gov/integrated-public-alert-warning-system>
- **Committee for Tactical Emergency Casualty Care (C-TECC):** The C-TECC develops guidelines and resources for casualty management during high-threat civilian tactical and rescue operations. TECC build off military battlefield guidelines of Tactical Combat Casualty Care and take into account the unique needs of the civilian medical and operational environments. <http://www.c-tecc.org>

Attachment C

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

44. With respect to the event(s) involving the release of gasoline or other petroleum product(s) in the vicinity of the Tunbridge Apartment complex on or about Monday, November 11, 2019,

- (a) Identify each and every product and the quantity of each such product that was released;

RESPONSE: Product released: Gasoline (non-ethanol)
Approximately 4.1 BBLS

DATE: January 13, 2020

BY: Office of Special Assistants

- (b) Explain in detail the methods by which you determined the quantities of product that were released;

RESPONSE: SPLP performed an engineering calculation and an mass balance calculation. See documents to be produced.

DATE: January 13, 2020

BY:

- (c) Explain the cause(s) of the release(s);

RESPONSE: The cause of the release was a tubing fitting that was part of the valve as provided by the manufacturer. Post-incident evaluation by the tubing vendor identified that the tubing fitting had not been assembled correctly by the manufacturer. The tubing was not inserted through the ferrule far enough which did not allow the ferrule to properly engage on the tubing.

DATE: January 13, 2020

BY: Matthew Gordon

- (d) State how long the release(s) continued before it or they were stopped;

RESPONSE: See Response to 44(l).

DATE: January 13, 2020

BY: Matthew Gordon

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

(e) Identify the area in which an odor was noticeable;

RESPONSE: The area in which the odor was “noticeable” depends on a variety of factors, including an individual’s ability to smell, which differs by person and may be subjective. SPLP cannot define a specific area in which any individual may have “noticed” the odor. SPLP is aware that persons up to approximately 500 feet said they noticed the odor.

DATE: January 13, 2020

BY: Matthew Gordon

(f) Explain in detail the efforts you or your agents made to inform government officials of the existence of the leak(s), including without limitation officials from Delaware County Emergency Services, the Pennsylvania Public Utility Commission, the Pennsylvania Department of Environmental Protection, Middletown Township, Pennsylvania Fish & Boat Commission, and the U.S. Coast Guard;

RESPONSE: SPLP called the following entities the night of the event: Pa PUC, PHMSA, County OEM, and PADEP. SPLP spoke with Middletown Township officials at the scene that night, as well as emergency responders and provided updates as the event was ongoing. See Response to 44(l). SPLP also utilized NRC reporting, which notified the following governmental agencies of the event on the evening of the event:

- CENTERS FOR DISEASE CONTROL (GRASP)
- DELAWARE COUNTY DES (EMERGENCY MGMT/HAZMAT RESPONSE TEAM)
- DELAWARE EMERGENCY MGMT AGENCY (MAIN OFFICE)
- DELAWARE STATE POLICE (MAIN OFFICE)
- DEPT OF HEALTH AND HUMAN SERVICES (SECRETARY'S OPERATION CENTER (SOC))
- DHS DEFENSE THREAT REDUCTION AGENCY (CHEMICAL AND BIOLOGICAL)
- DOT CRISIS MANAGEMENT CENTER (MAIN OFFICE)
- DELAWARE VALLEY INTEL CENTER (REGIONAL FUSION CENTER/PHILI PD)
- U.S. EPA III (MAIN OFFICE)
- FLD INTEL SUPPORT TEAM PHILADELPHIA (MAIN OFFICE)
- NATIONAL INFRASTRUCTURE COORD CTR (MAIN OFFICE)

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- NJ STATE POLICE (MARINE SERVICES BUREAU)
- NOAA RPTS FOR PA (MAIN OFFICE)
- NTSB PIPELINE (MAIN OFFICE)
- PA ENVIRONMENTAL PROTECTION AGENCY (EMERGENCY ENVIRONMENTAL RESPONSE)
- PA STATE POLICE (BUREAU OF CRIMINAL INVESTIGATION)
- PIPELINE & HAZMAT SAFETY ADMIN (OFFICE OF PIPELINE SAFETY (AUTO))
- PIPELINE & HAZMAT SAFETY ADMIN (OFFICE OF PIPELINE SAFETY)
- PIPELINE & HAZMAT SAFETY ADMIN (HAZARDOUS MATERIAL ACCIDENT INVESTIGATION)
- SECTOR DELAWARE BAY (COMMAND CENTER)
- SECTOR DELAWARE BAY (RESPONSE)
- DE DEPT OF NAT RES AND ENV CTRL (MAIN OFFICE)
- OFFICE OF ENV. POLICY & COMPLIANCE (MAIN OFFICE)
- PA EMERG MGMT AGCY (MAIN OFFICE)
- USCG DISTRICT 5 (D5 DRAT)

SPLP also notified Aqua, PA.

DATE: January 13, 2020

BY: Matthew Gordon

- (g) Explain in detail the efforts you or your agents made to inform the public contemporaneously what steps if any the public should take by way of precautions; and

RESPONSE: SPLP objects to this request to the extent it implies that contemporaneous with a pipeline incident it is SPLP's duty to inform the public what steps to take. See Response to Flynn Set I, No. 26. In sum, it is the local or county emergency response organization's duty to make that determination and inform the public. That is exactly what occurred here. EMS advised residents to shelter in place. During the incident, SPLP did receive calls from residents during the event, returned those calls, and visited a resident's home per that resident's request. See Responses to 44(l) and 44(h).

DATE: January 13, 2020

BY: Matthew Gordon

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- (h) Explain in detail the efforts you or your agents made after the event was over to inform the public via written notice or public media as to what had occurred and what concerns the public should have under the circumstances.

RESPONSE: SPLP objects to this request's implication that the public should have "concerns" after the event. SPLP issued the following statement to the Delco Daily Times, KYW radio, CBS3, ABC6, NBC, the Philadelphia Inquirer, and Bloomberg:

There was a small misting of gasoline this evening that was the result of a tubing leak on our 8 inch refined products line that runs through Middletown Township in Delaware County. The pipeline was shut in and the situation was quickly contained. While there is an odor, there is no risk to those in the area. The emergency response units that were on site confirmed that there is no impact to air quality. We expect the odor to dissipate as our crews work throughout the night to remediate the area.

DATE: January 13, 2020

BY: Lisa Coleman

- (i) Identify all persons, including emergency responders, who experienced any health effects in connection with the release(s) and its or their sequelae;

RESPONSE: SPLP is unaware of any person experiencing health effects in connection with the release or its sequelae.

DATE: January 13, 2020

BY: Matthew Gordon

- (j) For each person identified in response to (h) above, explain how that person came to experience health effects.

RESPONSE: N/A

DATE: January 13, 2020

BY: Matthew Gordon

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

- (k) For each person identified in response to (h) above, set forth the extent of that person's health effects and the treatment that person received.

RESPONSE: N/A

DATE: January 13, 2020

BY: Matthew Gordon

- (l) Set forth a detailed timeline of the entire release event, for each event, including but not limited to time the release commenced, when Sunoco became aware of it, how Sunoco became aware of it, when Sunoco personnel were dispatched to the scene, when Sunoco personnel arrived at the scene, the time when Sunoco first spoke with Delaware County Emergency Services, when Delaware County first responders first arrived, when the release was contained.

RESPONSE:

[BEGIN HIGHLY CONFIDENTIAL, CONFIDENTIAL SECURITY INFORMATION]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

• [REDACTED]

**Meghan Flynn, et al. v. Sunoco Pipeline L.P.
Consolidated Docket No. C-2018-300616 et al.**

Sunoco Pipeline L.P.'s Answers to Flynn Complainants' Interrogatories, Set 2

[END HIGHLY CONFIDENTIAL, CONFIDENTIAL SECURITY INFORMATION]

DATE: January 13, 2020

BY: Matthew Gordon

VERIFICATION

I, Matthew Gordon, hereby state that the facts above set forth are true and correct (or are true and correct to the best of my knowledge, information and belief) and expect to be able to prove the same at a hearing held in this matter. I understand that the statements herein are made subject to the penalties of 18 Pa. C.S. § 4904 (relating to unsworn falsification to authorities).

Date: February 18, 2020



Matthew Gordon
Senior Director of Liquid Pipeline Operations
Energy Transfer Partners

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a true copy of the forgoing document upon the persons listed below in accordance with the requirements of § 1.54 (relating to service by a party).

VIA ELECTRONIC MAIL

Michael S. Bomstein, Esquire
Pinnola & Bomstein
Suite 2126 Land Title Building
100 South Broad Street
Philadelphia, PA 19110
mbomstein@gmail.com

Counsel for Flynn et al. Complainants

Anthony D. Kanagy, Esquire
Garrett P. Lent, Esquire
Post & Schell PC
17 North Second Street, 12th Floor
akanagy@postschell.com
glent@postschell.com

*Counsel for Intervenor
Range Resources – Appalachia LLC*

Erin McDowell, Esquire
3000 Town Center Blvd.
Canonsburg, PA 15317
emcdowell@rangeresources.com

Counsel for Range Resources Appalachia

Margaret A. Morris, Esquire
Reger Rizzo & Darnall LLP
Cira Centre, 13th Floor
2929 Arch Street
Philadelphia, PA 19104
mmorris@regerlaw.com

*Counsel for Intervenor
East Goshen Township and County of Chester*

Rich Raiders, Esquire
Raiders Law
606 North 5th Street
Reading, PA 19601
rich@raiderslaw.com

*Counsel for
Andover Homeowner's Association, Inc.*

Vincent M. Pompo
Guy A. Donatelli, Esq.
24 East Market St., Box 565
West Chester, PA 19382-0565
vpompo@lambmcerlane.com
gdonatelli@lambmcerlane.com

*Counsel for Intervenor
West Whiteland Township,
Downingtown Area School District,
Rose Tree Media School District*

Leah Rotenberg, Esquire
Mays, Connard & Rotenberg LLP
1235 Penn Avenue, Suite 202
Wyomissing, PA 19610
rotenberg@mcr-attorneys.com

*Counsel for Intervenor
Twin Valley School District
James R. Flandreau
Paul, Flandreau & Berger, LLP
320 W. Front Street
Media, PA 19063
jflandreau@pfblaw.com*

*Counsel for Intervenor
Middletown Township*

Mark L. Freed
Joanna Waldron
Curtin & Heefner LP
2005 S. Easton Road, Suite 100
Doylestown, PA 18901
mlf@curtinheefner.com
jaw@curtinheefner.com

*Counsel for Intervenor
Uwchlan Township*

Josh Maxwell
Mayor of Downingtown
4 W. Lancaster Avenue
Downingtown, PA 19335
jmaxwell@downingtwn.org

Pro se Intervenor

James C. Dalton, Esquire
Unruh Turner Burke & Frees
P.O. Box 515
West Chester, PA 19381-0515
jdalton@utbf.com

*Counsel for West Chester Area School District,
Chester County, Pennsylvania*
Virginia Marcille-Kerslake
103 Shoen Road
Exton, PA 19341
vkerslake@gmail.com

Pro Se Intervenor

Thomas Casey
1113 Windsor Dr.
West Chester, PA 19380
Tcaseylegal@gmail.com

Pro se Intervenor

Patricia Sons Biswanger, Esquire
217 North Monroe Street
Media, PA 19063
patbiswanger@gmail.com

Counsel for County of Delaware

Melissa DiBernardino
1602 Old Orchard Lane
West Chester, PA 19380
lissdibernardino@gmail.com

Pro se Complainant

Joseph Otis Minott, Esquire
Alexander G. Bomstein, Esquire
Ernest Logan Welde, Esquire
Kathryn L. Urbanowicz, Esquire
Clean Air Council
135 South 19th Street, Suite 300
Philadelphia, PA 19103
Joe_minott@cleanair.org
abomstein@cleanair.org
lwelde@cleanair.org
kurbanowicz@cleanair.org

James J. Byrne, Esquire
Kelly S. Sullivan, Esquire
McNichol, Byrne & Matlawski, P.C.
1223 N. Providence Road
Media, PA 19063
jjbyrne@mbmlawoffice.com
ksullivan@mbmlawoffice.com

*Counsel for Thornbury Township, Delaware
County*

Michael P. Pierce, Esquire
Pierce & Hughes, P.C.
17 Veterans Square
P.O. Box 604
Media, PA 19063
Mppierce@pierceandhughes.com


Counsel for Edgmont Township

Rebecca Britton
211 Andover Drive
Exton, PA 19341
rbrittonlegal@gmail.com

Pro se Complainant

Laura Obenski
14 South Village Avenue
Exton PA 19341
ljobenski@gmail.com

Pro se Complainant



Thomas J. Sniscak, Esquire
Kevin J. McKeon, Esquire
Whitney E. Snyder, Esquire

Dated: February 18, 2020