

---

*A Publication for AGA and EEI Members*

Prepared by the AGA Natural Gas  
Security Committee – Physical Security  
Subcommittee

400 North Capitol St., N.W., Suite 450

Washington, DC 20001

Phone: (202) 824-7000

Web site: [www.aga.org](http://www.aga.org)

And

EEI Security Committee

701 Pennsylvania Avenue NW,

Washington, DC 20004

Phone: (202) 508-8000

Web site: [www.eei.org](http://www.eei.org)

**August 2021**

# **Suspicious Activity / Sabotage Prevention Resource Guide**

Copyright © 2021 American Gas Association

and Edison Electric Institute

All Rights Reserved

## **DISCLAIMER**

AGA and EEI disclaim liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of or reliance on AGA or EEI publications. AGA and EEI make no guaranty or warranty as to the accuracy and completeness of any information published therein. The information contained therein is provided on an “as is” basis and neither AGA nor EEI make any representations or warranties including any expressed or implied warranty of merchantability or fitness for a particular purpose.

In issuing and making this document available, AGA and EEI are not undertaking to render professional or other services for or on behalf of any person or entity. Nor are AGA or EEI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

AGA and EEI have no power, nor do they undertake, to police or enforce compliance with the contents of this document. Nor do AGA and EEI list, certify, test or inspect products, designs or installations for compliance with this document. Any certification or other statement of compliance is solely the responsibility of the certifier or maker of the statement.

AGA and EEI do not take any position with respect to the validity of any patent rights asserted in connection with any items that are mentioned in or are the subject of AGA and EEI publications, and AGA and EEI disclaim liability for the infringement of any patent resulting from the use of or reliance on its publications. Users of these publications are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Users of this publication should consult applicable federal, state and local laws and regulations. AGA and EEI do not, through its publications intend to urge action that is not in compliance with applicable laws, and its publications may not be construed as doing so.

***Copyright © 2021, American Gas Association and Edison Electric Institute, All Rights Reserved.***

## Suspicious Activity / Sabotage Prevention Resource Guide

AGA and EEI Security Committees have partnered together to provide a package of suspicious activity/sabotage prevention resources developed by AGA and EEI member companies related to behavioral recognition, training, reporting, and other relevant materials.

These documents are for reference only and are not intended to represent best practices on this subject. The contents of this resource package are detailed below.

### Table of Contents

1.	Sabotage Vandalism Report Template .....	4-5
	<i>One-page template for reporting physical and cyber sabotage</i>	
2.	Sabotage TTX .....	6-34
	<i>Sabotage table-top exercise</i>	
3.	Situational Awareness Training Deck .....	35-64
	<i>Field worker safety training slides</i>	
4.	Incident Reporting .....	65-71
	<i>Workforce incident reporting training slides</i>	
5.	Intelligence Requirements v2020 .....	72-77
	<i>Template on collecting threat intelligence</i>	
6.	Identifying Unusual Behavior Utility A .....	78-82
	<i>Guide for identifying suspicious or unusual behavior in the workplace</i>	
7.	Susp Activity, Threat and Sabotage Reporting .....	83-84
	<i>A process flow chart that illustrates the reporting process, key contacts, and response activities</i>	
8.	Susp Activity Recognition CBT Utility A .....	85-100
	<i>Training slides for field employees on how to identify suspicious behavior</i>	

# Document 1

## Sabotage Vandalism Report Template

One-page template for reporting physical and cyber sabotage

[Click here to return to the Table of Contents](#)

CORPORATE ADMINISTRATIVE PROCEDURE		
PLAN #	Reporting Procedure for Damage, Destruction, Physical Threats or Sabotage	Page 1 of 1
		Rev 2

Appendix 1, Reporting Procedure for Damage, Destruction, Physical Threats or Sabotage Events to an XXXXXXXX Facility

YOUR LOGO HERE

## Reporting Procedure for Damage, Destruction, Physical Threats or Sabotage events to an XXXXXXXX Facility

Last Revision Date June 23, 2014

Any **suspected or confirmed Damage, Destruction, Physical Threats or Sabotage events to an XXXXXXXX Facility** must be reported immediately to the XXXXXXXX Corporate Security Department.

For incidents in STATE call the  
Security Alarm Center at

For incidents in STATE call the  
Security Alarm Center at

Any **suspected or confirmed Cyber Sabotage Incident** must be reported immediately to the XXXXXXXX Service Desk at:

*While the details for recognizing and reporting damage, destruction, physical threats and sabotage events to an XXXXXXXX facility are provided inside this document, a thumb-nail summary is :*

**It is responsibility of Employee, Contractor and Service Vendor to immediately report damage, destruction, physical threats and sabotage events to an XXXXXXXX facility that may include:**

- Tampering with or vandalism of infrastructure of electric grid such as transmission towers, poles, transformers, substation equipment, gas valves, gas take-points, regulator stations, underground storage, telecommunications etc.
- Disrupting the fuel or water supply to a power generation plant or disrupting operations by false or substantiated threats (bomb, fire, biological hazard, etc.)
- Unexplained unlocked facility gates, doors, yard-cabinets or control houses
- Unauthorized people requesting sensitive information (through e- mails, phone calls) about security systems, operations, software, facility staffing, telecommunications, etc.
- Unauthorized people plugging devices into the data or telecommunications network
- Verbal or written threats targeting security systems, software, operations, or facilities
- Suspicious packages located at XXXXXXXX facilities
- New or unauthorized equipment in the vicinity of the cyber assets
- Workstations or laptops that start working in uncharacteristic manner

### **Responsibilities**

- Act with safety in mind
- Call the appropriate (Missouri or Illinois) Security Alarm Center
- Unless absolutely necessary for safety, do not to touch, walk through or disturb any type of evidence, until the proper authorities have arrived on scene to investigate
- Take notes – document who, what, where, when, why and how
- When possible, take photographs
- Also follow your Departmental procedures, if any, for responding to such incidents or events

# Document 2

## Sabotage TTX

Sabotage table-top exercise

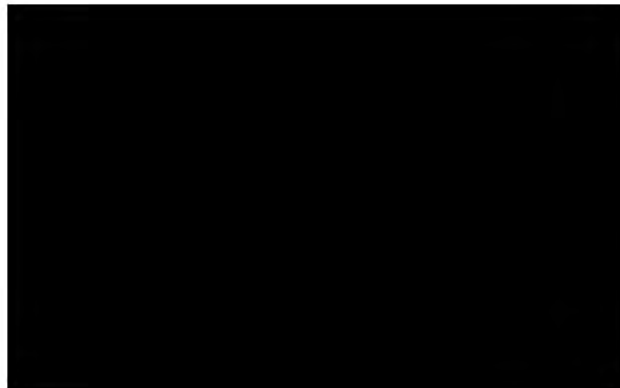
[Click here to return to the Table of Contents](#)



# Tabletop Response Drill

( [REDACTED] )

Sept. 5, 2019







# Drill Objectives

- ✓ **Familiarize yourself with your roles and responsibilities during a significant crisis event faced by the company**
- ✓ **Recognize notification/communications elements that are used during a crisis event**
- ✓ **Reinforce & understand roles and integration of various company levels & support functions**
- ✓ **Assess support capabilities to field/incident responders**
- ✓ **Foster teamwork and an understanding of the entire response organization**





# Ground Rules

- **The Tabletop Drill will “stay in this room” including online participants and will involve discussion only**
- **All present should actively participate**
- **The focus should be on discussing resources, needs and high-level actions, remember this is more about “strategy” not “tactics” !!!**
- **Necessary notifications to outside parties should be discussed and noted**
- **Participants should be prepared to discuss key needs & actions of their functions**



# Incident Overview/Conditions

- **Numerous calls are coming into Call Center complaining of strong gas odors near company Border Station [REDACTED] in [REDACTED]**
- **Weather conditions are normal for this time of year, with today's temperature currently at 71 degrees and a forecasted high of 82 degrees**
- **Winds today are brisk, blowing out of the SE at 15 mph, with gusts up to 25 mph**







# Situational Update – 9:07 a.m.



- The Call Center receives a call from a “private number” claiming responsibility for **“causing a big problem at the border station at [REDACTED] Street and [REDACTED] Rd.”**
- The caller adds **“You can trust old Buddy when I tell you that I know what I’m doing, and that this isn’t the end of this”** then abruptly hangs up.
- Calls from customers and local residents are beginning to escalate; with some calls also describing a “buzzing drone” flying over the area





# What are your response actions?







# Situation Update – 9:22 a.m.

- Personnel from the company's [REDACTED] Office have just arrived at the Border Station
- They report a high concentration of odorant smell all around the area and are beginning to perform leak surveys
- As of 9:20 a.m., Customer Service has received over 100 calls inquiring as to whether there is a gas leak
- Local authorities have also contacted the company wanting to know what is going on?
- Gas Control HAS NOT noted any significant drops in pressure in its SCADA readings or any applicable alarms
- The Call Center has contacted Corporate Security about the anonymous call which came from a "blocked" number
- Since the facility is where [REDACTED] distribution and transmission lines from [REDACTED] converge, there is some confusion as to which lines/facilities may be affected ([REDACTED])



# What are your response actions?







# Operational Discussion

- **What would be our process for responding operationally to this incident?**
- **How would we investigate this?**
- **How long will it take to “get a read” on what is going on and how many personnel would have to be involved at the site?**
- **What are our options?**
- **What are the impacts to customers?**
- **Are there any current risks to human safety?**
- **What, if any special safety steps should our personnel be taking?**
- **Are we working within the ICS structure?**
- **Who is in charge?**





# Situation Update – 9:56 a.m.



- **Personnel at Border Station [REDACTED] report that there is no evidence of a gas leak; rather the problem seems to be coming from an unknown source of mercaptan (odorant)**
- **Over 400 calls -- many from fearful, annoyed, or impacted residents -- have come into Customer Service in the past hour**
- **Units from [REDACTED] Fire & Rescue Station #12 are now coordinating with [REDACTED] responders at the site**
- **The Incident Command Post has been established about 400 yards south (downwind) of the [REDACTED] border station, near the junction [REDACTED] St. & [REDACTED] Dr at [REDACTED] parking lot.**
- **[REDACTED] Public Safety Director [REDACTED] is at the scene and wants advice from company personnel as to whether to call for an evacuation of nearby homes & businesses**





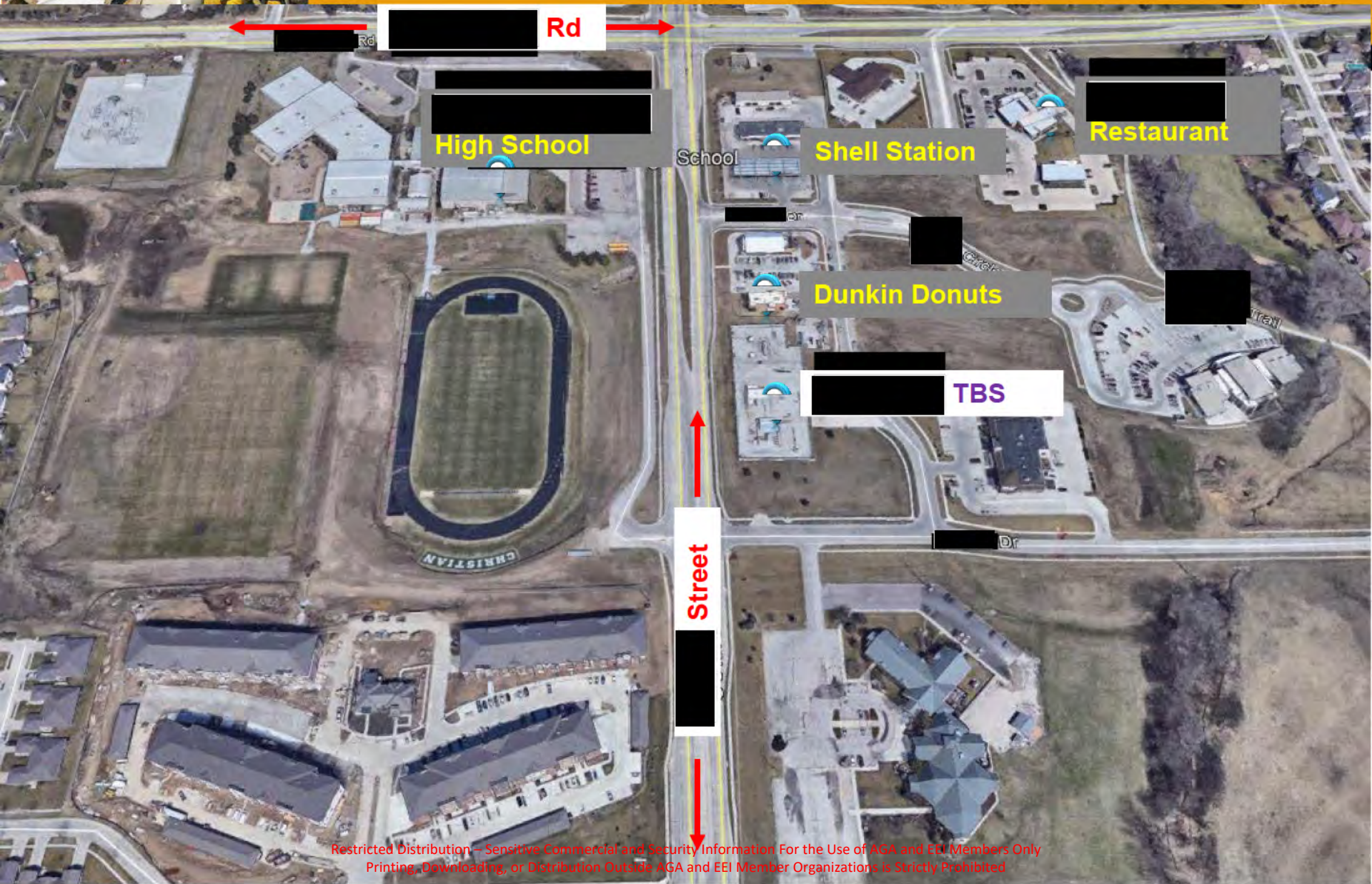
# What are your response actions?







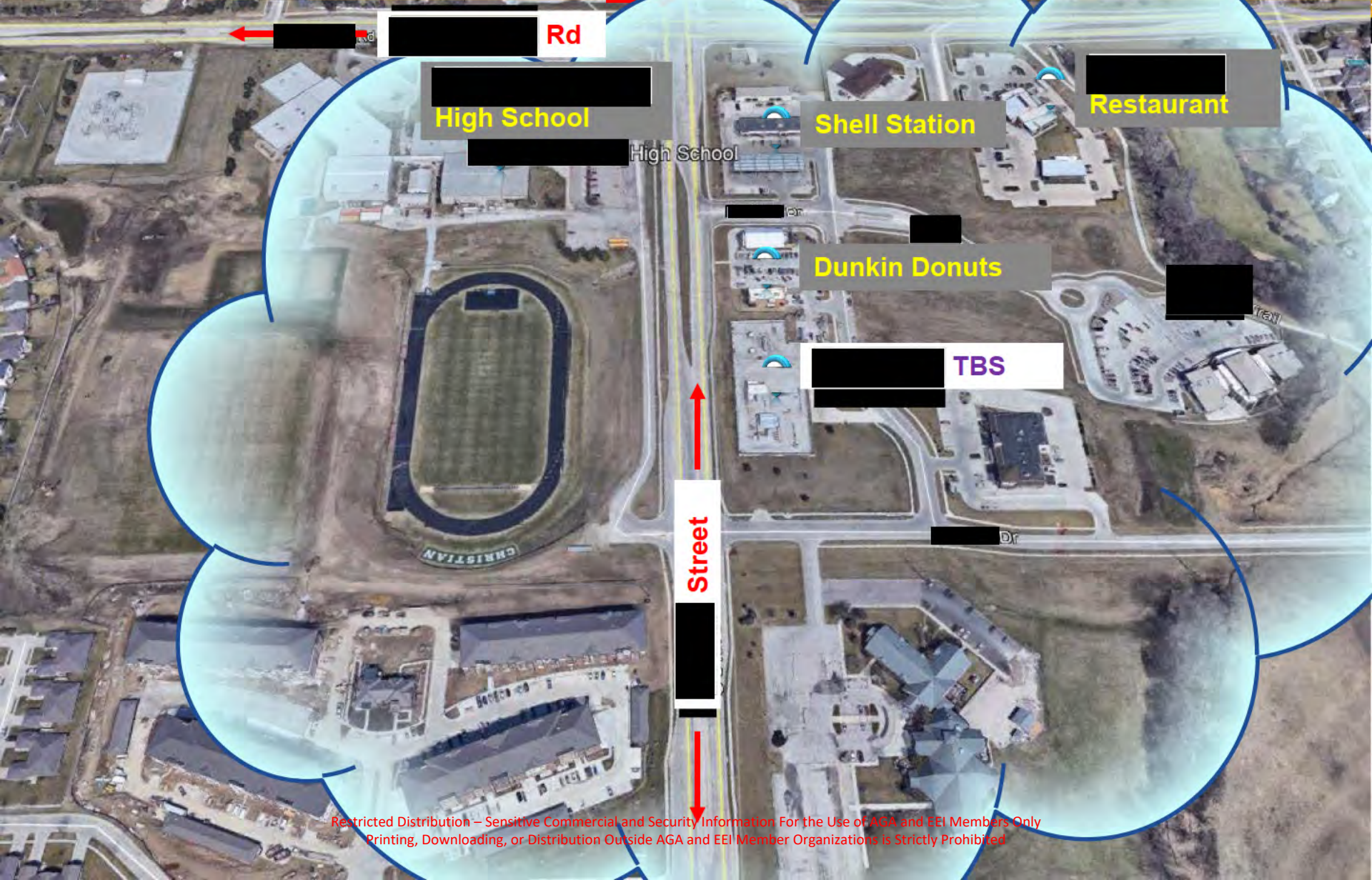
# Incident Site







# Incident Site/Area







# Situation Update – 10:20 a.m.

- A news helicopter from [REDACTED] in [REDACTED] is now hovering over the area and numerous media inquiries are being made to the [REDACTED] Office and Call Center as news outlets are calling phone numbers on pipeline markers and facility signage
- Local TV outlets have interrupted normal programming to report “live from the scene”
- TV coverage includes interviews with nearby residents, many of whom report they are ill or having various health issues: headaches, nausea, difficulty in breathing, etc.
- Social media commentary is also extensive, with numerous posts on Facebook, Twitter and several videos now on YouTube
- The [REDACTED] County Sheriff’s office is facilitating an evacuation of a one-mile radius of the border station







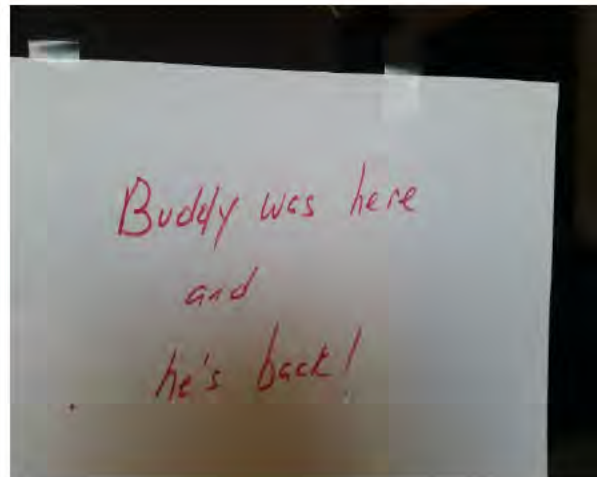
# What are your response actions?





# Situation Update – 10:35 a.m.

- [REDACTED] personnel at the site now report finding several hand-written signs in red ink at Border Station [REDACTED]
- One sign, found taped inside of an Odorizer control panel at the facility says, "**Buddy Was Here and He's Back!**"
- The other signs say "**It's not about money, it's about sending a message. Everything Burns!**" and were found at various locations in and around the Border Station
- Several eyewitness told local media and emergency responders that a drone buzzing back and forth over the site also dropped some playing cards that said "**Joker Ha Ha Ha**"



Found Joker Card



# What are your response actions?







# Situation Update – 10:55 a.m.



- The evacuations and road closures are snarling traffic in the region
- Local shelters for evacuees are being set up at [REDACTED] Middle School – Address [REDACTED] Dr.
- According to press reports, two [REDACTED] hospitals are reporting admissions due to respiratory issues
- One TV crew has requested a live interview with [REDACTED] personnel
- Several employees have mentioned to Operations' management their belief that the "Joker" and "Buddy" references left at the scene may be linked to a recently terminated employee [REDACTED] "Buddy" [REDACTED]



# What are your response actions?







# Situation Update – 11:20 a.m.

- An explosion just occurred at a shared company border station [REDACTED]
- The [REDACTED] is currently on fire, but no injuries to personnel or local residents are being reported
- Corporate Affairs/Communication staff report that a Facebook page entitled “Buddy Boy” shows pictures of [REDACTED] Border Station [REDACTED], including photos with the handmade signs “**Buddy is Back!**” posted on equipment
- Links on the page include sites protesting the Keystone/TransCanada Pipeline and a “Friends” link to [REDACTED] Facebook page







# What are your response actions?





# Situation Update – 12:15 p.m.



- Emergency personnel at [REDACTED] have responded to the affected facility and have the fire under control and nearly out
- A mysterious backpack, with an attached **"Joker"** playing card was just found at a third company facility in [REDACTED] at the [REDACTED] Station [REDACTED] that serves over 30K Customers
- Back in [REDACTED], coverage of the odorant issue predominates [REDACTED] newscasts, and several media outlets are now asking whether "The Joker" is someone affiliated with [REDACTED]
- One local resident and gas customer, [REDACTED], has been on news reports holding a Joker playing card found in a nearby Dunkin Donuts parking lot, and stating "I just pray that this isn't terrorists !"





# What are your response actions?



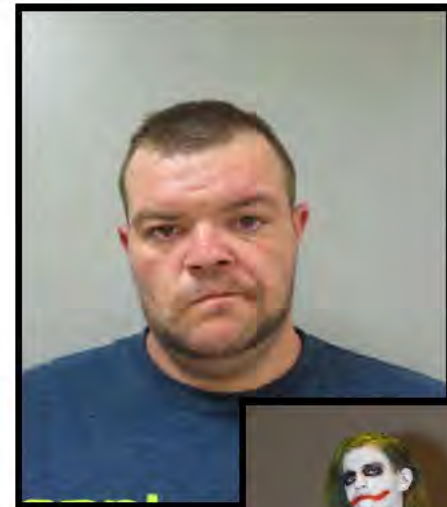




# Situation Update – 12:40 p.m.

**HR provided the following background on “Buddy” [REDACTED]:**

- After numerous warnings Buddy was terminated for poor performance, specifically because he was constantly on social media and the internet during work hours as well as violating multiple [REDACTED] policies
- Buddy was deemed “highly proficient in his knowledge of operations” by his immediate and past [REDACTED] supervisors within [REDACTED]
- [REDACTED] vehemently denied the accusations leading to his discharge, saying this would “stain my name” and vowing that he would “make the company pay” for what they had done
- At that time, local management and HR assumed that [REDACTED] was threatening a lawsuit
- Co-workers also stated that [REDACTED] was “sympathetic” to recent pipeline protests in [REDACTED]; was “fascinated by drones” and had once dressed up as the Joker from the movie Batman at an after-work Halloween Party





# What are your response actions?







# Situation Update – 1:05 p.m.

- In [REDACTED], the odorant situation has now subsided and the authorities have lifted the evacuations as residents return to their homes
- A drone wreaking of odorant was just found crashed on a remote road outside of [REDACTED] by Police
- In [REDACTED] the fire is now out, but reports are that a nearby farmer in his 70s may have suffered a heart attack during the explosion
- This gentleman, [REDACTED], has been transported to the local hospital
- At the [REDACTED] location with the mysterious backpack, responders with expertise are dealing with possible explosives and have now arrived on scene







# What are your response actions?





# High-Level Drill Debrief

## Discussion Items

- ❑ Given the far-flung geographic footprint of this scenario, how well did our various groups work together?
- ❑ How was communication and access to critical information?
- ❑ Do you know your role?
- ❑ Do you understand our plan/structure?
- ❑ What issues do you see in our response capabilities based on this scenario?
- ❑ Based on this incident, what problems must we address?



# Document 3

## Situational Awareness Training Deck

Field worker safety training slides

[Click here to return to the Table of Contents](#)



# The importance of knowing your surroundings

Situational awareness and de-escalation training

# Safety minute



*Nothing* is more important than safety. Your safety and the safety of those we serve.

# Safety means being prepared

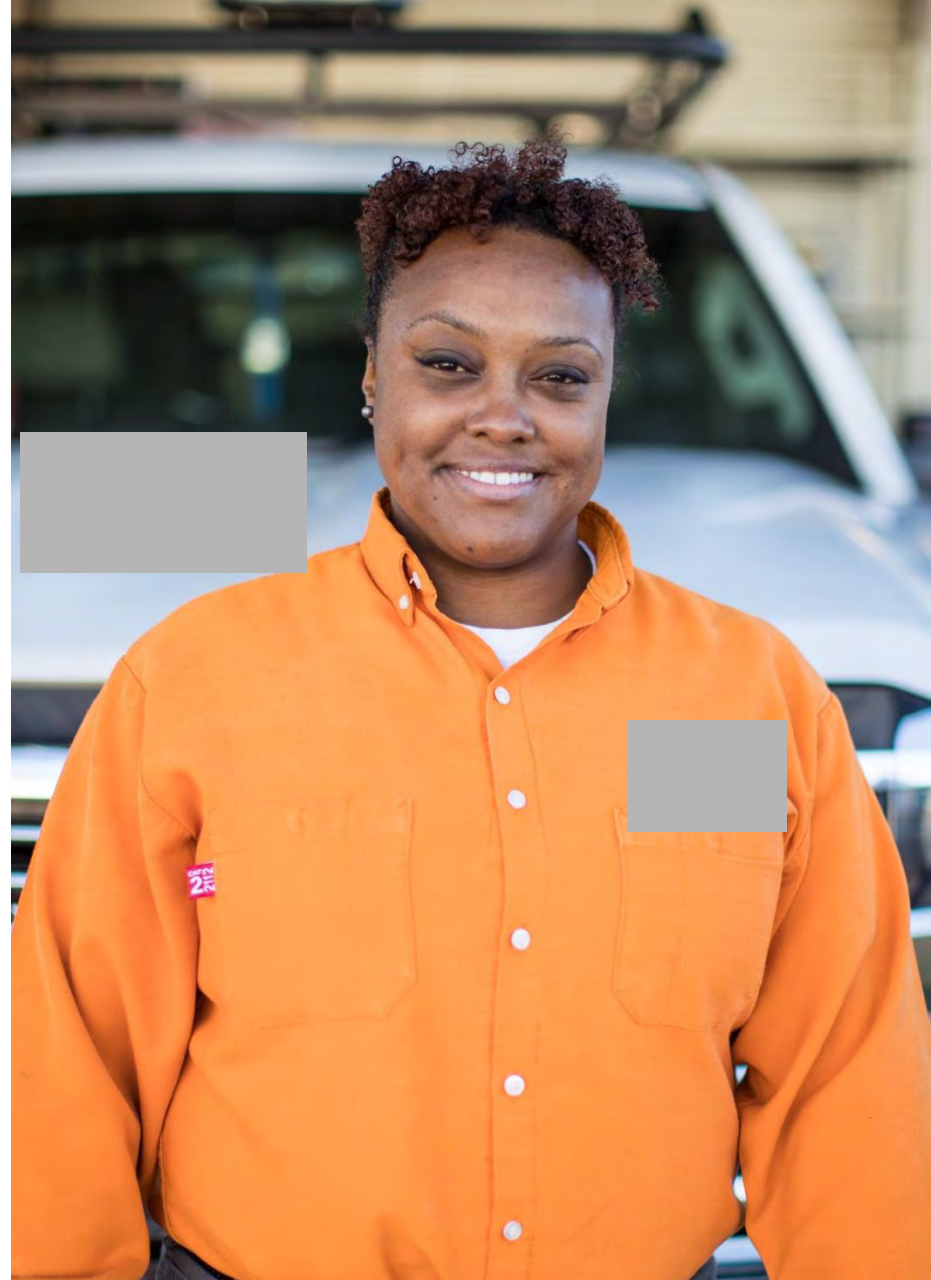
Your safety and the safety of our contractors and customers is our priority. So we are committed to training and preparing you to be as safe as possible.

- Our goal is to provide all employees and contractors with the knowledge they need to handle those who are hostile or dangerous.
- Field workers are on the frontlines. If a customer is upset, hostile or agitated, field workers can become the focus of that aggression. To address this issue, **we've developed a threat protocol.**
- Customer service representatives also deal with hostile and threatening customers. So an in depth threat protocol system has been established for them as well.



# What we'll learn today

- Situational awareness and how to use it
- Avoidance and the use of de-escalation skills
- Tools you can use to stay safe at work and home



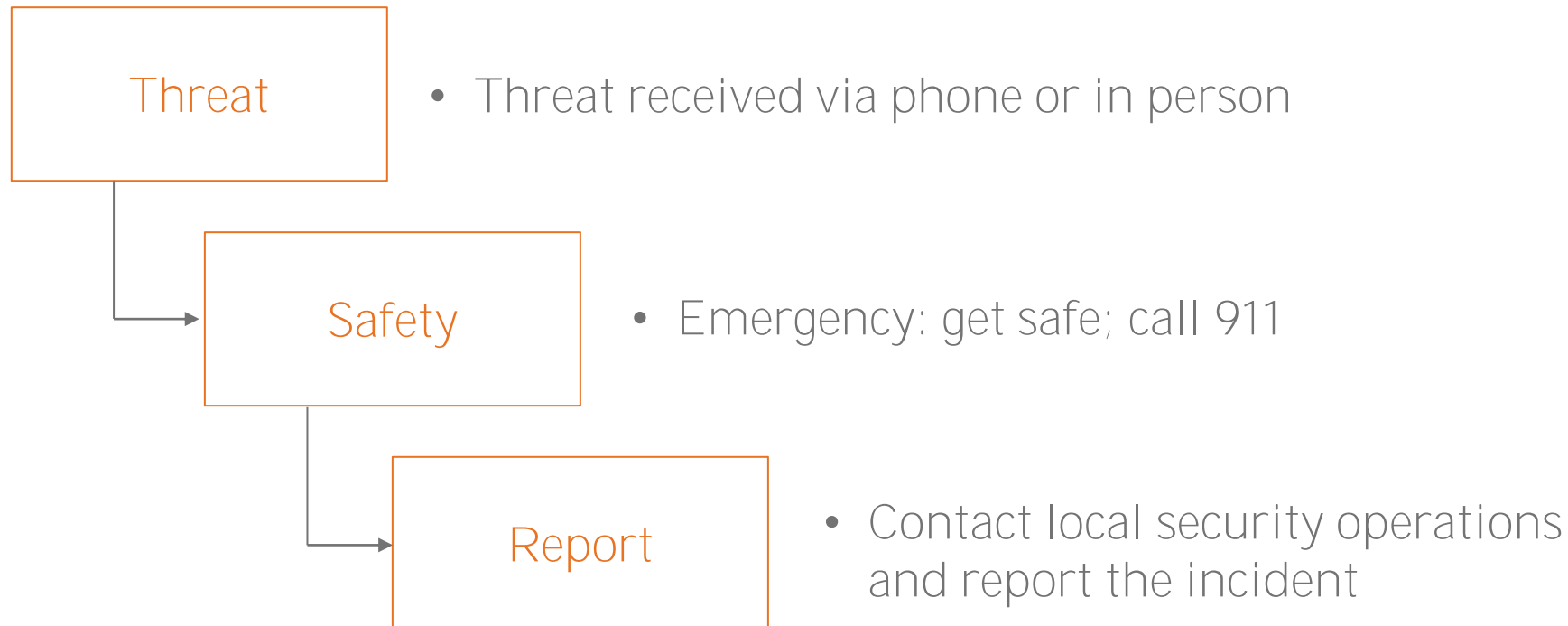
# The challenges of personal safety and security

When you're anywhere where you can be recognized as a  employee or contractor, you could be faced with challenges.

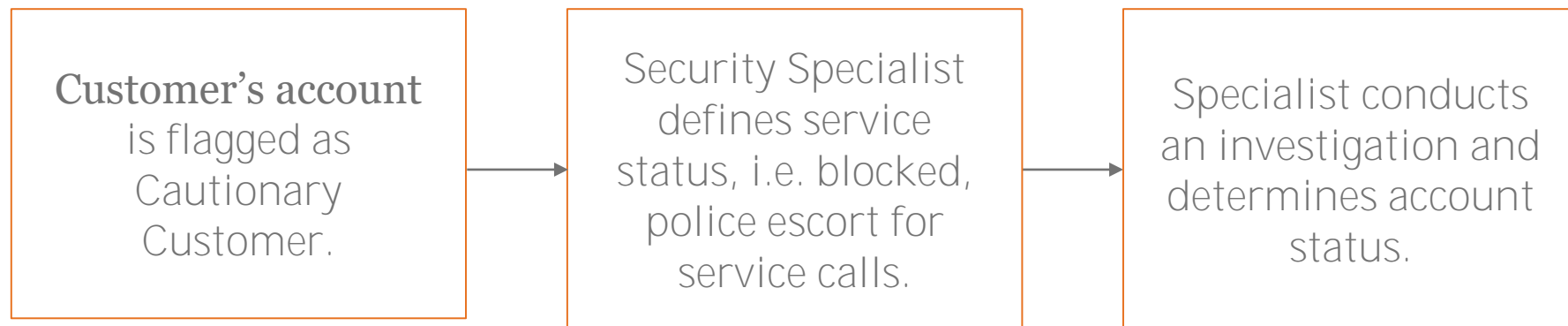
- Customers are angry at the company
- Someone is upset about a disconnection
- A customer is without gas and is feeling slighted
- Someone feeling like you are trespassing on their property
- A violent situation that has nothing to do with you or the company, but could still present danger



# Overcoming challenges with protocol



# Overcoming challenges with protocol





Identifying threats and  
knowing to use our protocol  
through situational awareness

# Situational awareness defined

- Understand your environment
- **Ask yourself, “What belongs and what doesn’t?”**
- Note if anything has changed or stayed the same
- Remember that nothing is the same
  - Not all people are the same
  - Not all situations are the same
  - Not all houses and yards are the same



# Become familiar with the situational awareness mindset

- Get in the right mindset when interacting with customers
- Stay tuned in
- Develop discipline around awareness





# Test your awareness



# Improve your awareness

- Know what belongs, and what doesn't
- Pay attention to the changes
- Notice anomalies
- Be proactive

## Look

What is happening?

## Think

What will happen next  
and how will it affect me?

## Act

Identify a hazard  
then act upon it

# Trust your gut

“The only real valuable thing is intuition.”

—Albert Einstein

- Intuition
- Instinct
- Funny feeling
- 6<sup>th</sup> sense
- Gut feeling
- “Spidey” sense



# Know what intuition is



Intuition is  
knowing without  
knowing why.



It is one of  
your fastest  
observation  
tools.



It is your early  
warning.

# Check your surroundings in advance

1. Know the area or residence in advance
2. Survey the area prior to parking
3. Park smart
4. Pay attention to your approach
5. Position yourself strategically
6. Look and listen



# Notice subtle behaviors

- Clinching fists
- Tightening of jaw
- Sudden change in body language
- Sudden change in vocal tone or volume
- Pacing
- Fidgeting
- “Rooster stance”
- “o-60”





# Putting situational awareness into practice

## Learn from real-life situations

- Tech approached a residence and was told by a subject on the porch not to come any closer. The tech hesitated. The subject became intimidating and sternly told the tech he was interrupting his business and not to come back. Observing his body language, and noticing his voice change from a normal tone to a stern voice, the tech became concerned for his safety and left the area.
- Supervisor received a complaint and upon responding to speak with the customer, the customer began screaming and cursing at the supervisor; blaming [REDACTED] for her water leak. During her verbal abuse, two males exited the same residence and also began cursing at the supervisor.
- Tech informed the customer of leaks and that service could not be restored. The **irate customer blocked the door and told the tech that he wasn't leaving until** service was restored. Tech told the customer he had to get his phone from his vehicle to contact his supervisor; the customer allowed him to pass. Once outside, the tech entered his vehicle and fled the area.

# Counteract behavior with de-escalation

- Use names
- Listen
- Avoid clichés
- Be nonjudgmental
- Continue to reassess the situation in order to respond effectively





# Improve your de-escalation skills

- Always be in control of yourself.

Appear calm. Relax your facial muscles. Use a low monotonous tone. Do not be defensive. Be respectful. Do not smile or touch.

- Be aware of your physical stance.

Stay at the same eye level. Allow extra space between each other. Stand at an angle, not full front to the subject. Do not maintain constant eye contact. Do not point or shake fingers. Keep hands out of pockets.

- Have a de-escalation discussion.

Calmly bring the situation down to baseline. Do not answer abusive questions. Explain limits and rules. Be empathetic. Do not ask how a person is feeling or analyze their feelings. Do not argue or try to convince.

# Deal wisely with angry people



# Learn from the experts

## Dr. Christian Conte: How to de-escalate someone

- Validate.

Acknowledge and recognize how the person feels. No one is right or wrong about how they feel; they have a right to feel how they do. Validate that they actually feel heard.

- Help people find options.

We all have choices. Help people explore their options. Anger leads to seeing only **what they're focused on; help them widen their perspective and see beyond the** problem so they can understand their options.

- Allow for choice.

Help people recognize their freedom of choice and that you will respect what they choose.



# Know what not to do when de-escalating



# Be prepared for challenges

- Distractions
- Complacency
- Normalization of deviance
- Tunnel vision

Quote from Culture of Safety (Duke University Medical Center):

**“System flaws set up good people to fail. 80% of errors are system induced. People often find ways of getting around processes which seem to be unnecessary or which impede the workflow. This is known as normalization of deviance.”**

# Escape when needed

- Avoid a violent or threatening customer as soon as you see the danger signs
- **You have permission to retreat. If you don't feel safe, leave**
- Use de-escalation to get out
- Remain calm, control your own behavior and use non-threatening body language
- If threatened with a weapon or assaulted, get to safety and call 911
- Once safe, contact your supervisor, then your local Security Operations Center



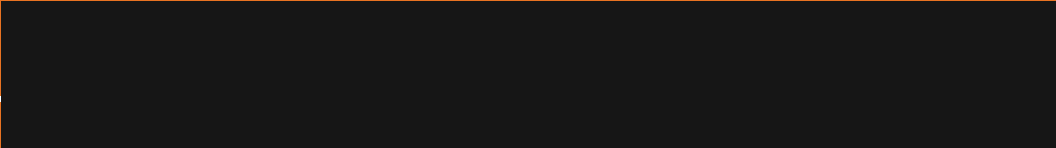
Have a plan B

What's YOUR plan B?

Stay prepared—always



“My greatest hope is that *every* employee returns home safely at the end of **the day.**”





# Document 4

## Incident Reporting

Workforce incident reporting training slides

[Click here to return to the Table of Contents](#)

# Incident Reporting

# Incident Reporting-Why we need incident reports:

The purpose of an incident report is to document and track workplace incidents. Why is this important?

- Events can identify issues or patterns that might easily be resolved by analysis of data
- The incident report serves as an official record of events,
- We have documentation which can be used for any follow up investigation involving criminal activity, or other internal matter

Any event relating to the security of [REDACTED] employees, its facilities or criminal activity should be reported to Corporate Security. Corporate Security will document the incident on an incident report form and conduct a follow-up investigation if needed.



# Incident Reporting

[Redacted]		SECURITY	
[Redacted]		[Redacted]	

Region:	Report Number:	Date:
---------	----------------	-------

Law Enforcement Complaint Number:	Reported By: Employee Name/Title/Number	Reported To: Name/Title/Number
--------------------------------------	--	--------------------------------

Incident Information			
Date Occurred:	To	Time Occurred:	To
Date/Reported:	Time Reported:	Site Name/Type:	
Incident Address:			

Type of Incident	
1.	
2.	
3.	

Reporting Party		
Name:	Race/Sex:	DOB:
Address:	Phone Number:	
Party Information:	Alt. Phone Number:	

Victim Information	
Name:	Race/Sex/DOB:
Address:	Phone Number:
Account Information:	
Name:	Race/Sex/DOB:
Address:	Phone Number:
Account Information:	

Witness Information		
Name:	Race/Sex:	DOB:
Address:	Phone Number:	
Party Information:	Alt. Phone Number:	

Suspect Information				
Name:	Race/Sex:	DOB:		
Address:		Phone Number:		
HGT:	WGT:	Build:	Eyes:	Hair:
Clothing:				
Account Information:				

Property Information		
Brand:	Model:	Serial #:
Property Description:		
Color:	Quantity:	Value:
Owner:		

Vehicle Information				
Year:	Make:	Model:	Type:	
Color:	Plate No:	Plate State:	Plate Year:	
VIN:	Vehicle Number:			
Vehicle Owner:				
Describe Damage:				

Narrative
-----------

Approval Process	
Prepared by:	Employee Number:
Reviewed by:	Employee Number:
Approved by:	Employee Number:

Resolution of the Incident		
Status:	Approved for File?	Referred to LEA:
Corporate Security Approval:	Date/Time:	

Recommendation
----------------

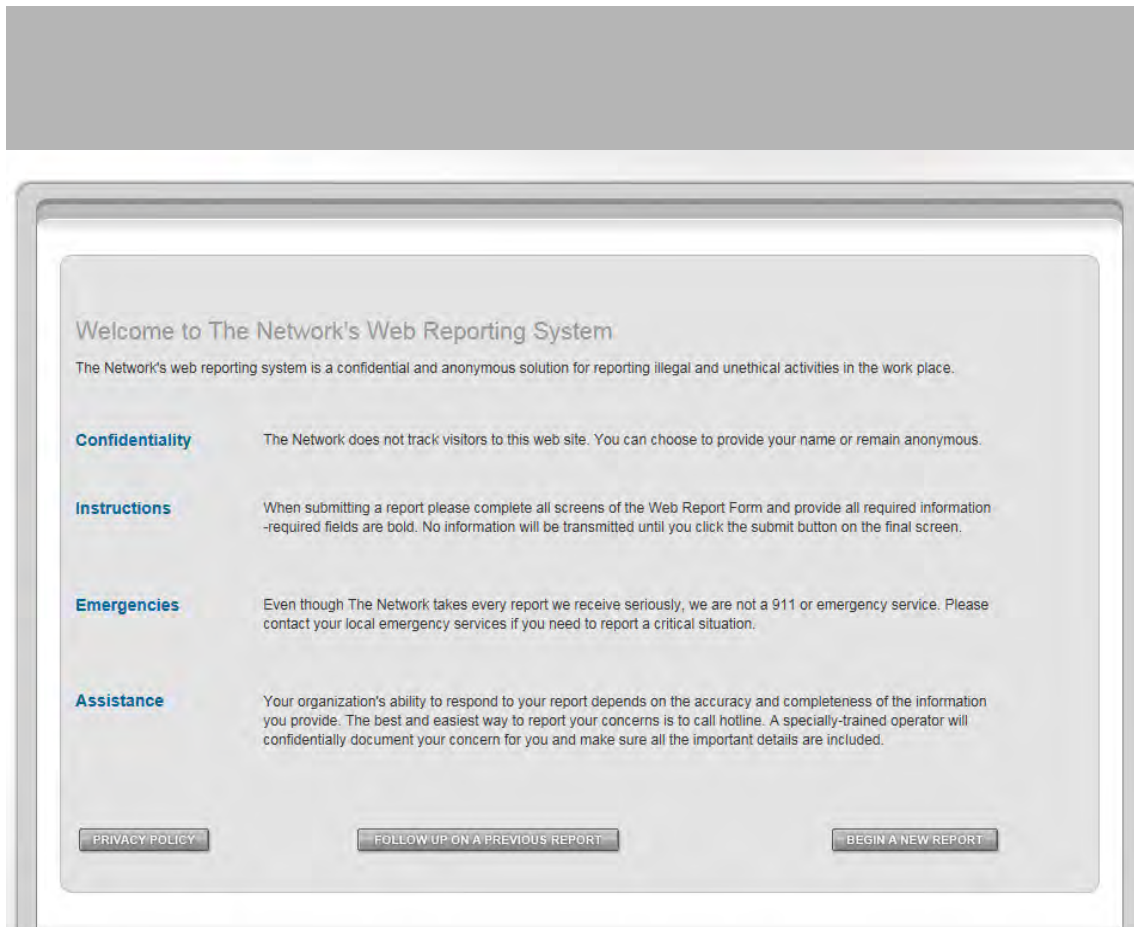
# Incident Reporting-Methods of Reporting

Contact the appropriate Security Operations Center by phone  
or email:



# Incident Reporting-Methods of Reporting

In cases where the confidential hotline reporting procedure may need to be followed, use the [REDACTED] email address or call toll free [REDACTED]



The screenshot displays a web page titled "Welcome to The Network's Web Reporting System". The page is designed with a light gray background and a white central content area. At the top, a header bar contains the title. Below the header, a paragraph explains that the system is a confidential and anonymous solution for reporting illegal and unethical activities in the workplace. The main content area is organized into four sections, each with a blue header and a descriptive paragraph: "Confidentiality" (explaining that the network does not track visitors), "Instructions" (detailing the reporting process and required information), "Emergencies" (clarifying that the network is not a 911 service), and "Assistance" (stating that the organization's response depends on the accuracy of the information). At the bottom of the page, there are three buttons: "PRIVACY POLICY", "FOLLOW UP ON A PREVIOUS REPORT", and "BEGIN A NEW REPORT".

Welcome to The Network's Web Reporting System

The Network's web reporting system is a confidential and anonymous solution for reporting illegal and unethical activities in the work place.

**Confidentiality** The Network does not track visitors to this web site. You can choose to provide your name or remain anonymous.

**Instructions** When submitting a report please complete all screens of the Web Report Form and provide all required information -required fields are bold. No information will be transmitted until you click the submit button on the final screen.

**Emergencies** Even though The Network takes every report we receive seriously, we are not a 911 or emergency service. Please contact your local emergency services if you need to report a critical situation.

**Assistance** Your organization's ability to respond to your report depends on the accuracy and completeness of the information you provide. The best and easiest way to report your concerns is to call hotline. A specially-trained operator will confidentially document your concern for you and make sure all the important details are included.

[PRIVACY POLICY](#) [FOLLOW UP ON A PREVIOUS REPORT](#) [BEGIN A NEW REPORT](#)

# Incident Reporting

## What should be reported?

- Assaults
- Threats
- Robbery
- Thefts
- Suspicious Person(s)
- Auto accidents
- Sick Case
- Accidental Injuries
- Workplace Violence





# Document 5

## Intelligence Requirements v2020

Template on collecting threat intelligence

[Click here to return to the Table of Contents](#)



# THREAT INTELLIGENCE GROUP: INTELLIGENCE REQUIREMENTS

Current as of October 23, 2020

The Threat Intelligence Group (TIG) delivers short- and long-term security intelligence to provide insight to [REDACTED] business leaders and security operations regarding potential and actual security threats to allow appropriate tactical and strategic directions to be established. Compiled and analyzed information informs policy and guides decisions for operational plans and mitigation strategies. Intelligence is gathered and informed by government, industry, and other open sources and converted into actionable information. The following categories outline, but are not limited to, the types of information of interest to the TIG and is requested to be reported to the TIG as soon as possible (noting that the TIG is not an operational response team). Attention to detail is crucial to the analysis of security information; reporting should include all pertinent information, including date, time, location, and any other descriptive information available.

## Intelligence Requirements (Physical or Cyber)

### Acquisition of Expertise

Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person and that could be used to threaten [REDACTED] assets and personnel.

### Activism

Environmental or any activism that otherwise impacts [REDACTED] assets through disruption, direct action, or other security incident.

### Aviation Activity

Operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property. May or may not be in violation of Federal Aviation Regulations.

- Includes activity involving Unmanned Aerial Systems (UAS; drones), with or without operator identification or location, that could pose a security risk to a [REDACTED] asset.

### Breach/Attempted Intrusion

Unauthorized personnel attempting to enter or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor). Unauthorized attempts to access [REDACTED] information assets, including applications (on premise or cloud hosted), network devices, servers, databases, end user devices, and the data stored within those environments.

TLP: WHITE

CONFIDENTIAL: NOT FOR EXTERNAL RELEASE WITHOUT APPROVAL BY [REDACTED] THREAT INTELLIGENCE

Threat Response and Analysis Center  
[REDACTED]





## Cyber Attack

Compromising or attempting to compromise or disrupt an organization's information technology (IT) or operational technology (OT) infrastructure. For more detail, see the Cyber Security Intelligence Requirements detailed below.

## Eliciting Information

Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.

## Expressed or Implied Threat

Communicating a spoken or written threat (electronic or hard copy) to damage or compromise a facility/infrastructure.

- Includes threats of damage or destruction against [REDACTED] facilities and assets, including threat toward employees.
- Includes threats made by [REDACTED] employees.
- Does not include customer threats to employees, in general.

## Materials Acquisition/Storage

Acquisition of unusual quantities of precursor materials, such as cell phones, pagers, fuel, and timers, such that a reasonable person would suspect possible criminal activity.

## Misrepresentation

Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover or conduct possible illicit activity.

- Includes impersonation of [REDACTED] employees as well as employees misrepresenting job function in order to gain access to a facility or other purpose intended to breach security.
- Includes impersonation of [REDACTED] websites and other externally facing applications.

## Observation/Surveillance/Reconnaissance

Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious.

- Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
- Overt or otherwise suspicious inbound/outbound network traffic (see Cyber Intelligence Requirements - Suspicious inbound/outbound traffic)
- Does not include Aviation type surveillance (see Aviation Activity requirements)

## Photography

Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person.

TLP: WHITE

CONFIDENTIAL: NOT FOR EXTERNAL RELEASE WITHOUT APPROVAL BY [REDACTED]

THREAT INTELLIGENCE



- Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

## Recruiting

Building operations teams and contacts, personnel data, banking data, or travel data.

## Sabotage/Tampering/Vandalism

Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.

- Instances of broken fences and attempts to break into facilities that cause identifiable damage are reported in this category.
- Includes damage to [REDACTED] infrastructure by gunfire or explosion.
- Includes damages (e.g., defacement) to [REDACTED] websites and other externally facing applications.

## Testing of Security

Interactions with or challenges to installations, personnel, or systems that reveal physical personnel or cybersecurity capabilities.

## Theft/Loss/Diversion

Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified] that are proprietary to the facility).

- Metal/Copper Theft: Specifically identifies that there was a security breach that led to a metal theft.
- Stolen [REDACTED] equipment: Any equipment that is damaged, lost, or stolen due to a physical security incident, including company phones, computers, other electronics, and access and identification badges.
- [REDACTED] information and data: Any data stolen, lost, destroyed or otherwise rendered unusable.

## Additional Cyber Intelligence Requirements

### Credential Misuse

Any prohibited or suspicious (likely malicious actor) use of [REDACTED] user account credentials indicative of network compromise. This can include unusual logins (time, location), unauthorized account creation, deletion, or privilege changes.

### Denial of Service (DoS) or Distributed Denial of Service (DDoS)

Any technique used to render a [REDACTED] information technology (IT) or operational technology (OT) resource unavailable to intended users by disrupting services of a host<sup>i</sup> connected to the internet or intranet.

<sup>i</sup> A host is any hardware device with access to a network, including computers and other electronic devices.

TLP: WHITE

CONFIDENTIAL: NOT FOR EXTERNAL RELEASE WITHOUT APPROVAL BY [REDACTED] THREAT INTELLIGENCE





## Website Clones

The existence of fraudulent websites, such as throughout typosquatting, intended to appear as legitimately owned and operated by [REDACTED], including for:

- Disseminating misinformation about [REDACTED]
- Infecting visitors with malware
- Obtaining sensitive employee or customer information such as login credentials

## Malware

Malicious code propagating on any [REDACTED] device or network. This includes both information technology (IT) and operational technology (OT).

## Phishing

Fraudulent emails portrayed as coming from trusted sources intended to facilitate other malicious cyber activities, such as malware downloads or solicitation of sensitive information. Phishing email(s) with the following characteristics should be reported:

- Impersonates [REDACTED] employees, including Executives (attempted or successful)
- Impersonates [REDACTED] targeting customers or vendors (attempted or successful)
- Impersonates vendor targeting [REDACTED] (attempted or successful)
- Spearphishing attempts especially against [REDACTED] officers (also known as whaling), super users, or critical infrastructure operators and support staff
- Uses energy sector themes to target [REDACTED], either through sender or content
- "Other" – any other noteworthy phishing email, due to its sophistication or other unique traits

## Supply Chain Compromise

The manipulation of products or product delivery mechanisms prior to the receipt by [REDACTED] for the purpose of system or process compromise.

## Suspicious Inbound/Outbound Traffic

Any network activity indicative of possible malicious activity. This includes, but is not limited to:

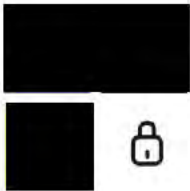
- Network/port scanning against [REDACTED] networks of interest. Specific examples:
  - Scanning outside of normal activity
  - Any scanning from indicators of compromise (IOC) associated with Advanced Persistent Threat (APT) actors
- Command and Control (C2) call ins/callbacks
- Suspicious interaction attempts against remote access solutions
- Other network traffic deemed suspicious

When activity is discovered meeting any of this criteria, Threat Intelligence specifically requests the following additional details:

- Dates/times of scanning
- Ports scanned

TLP: WHITE

CONFIDENTIAL: NOT FOR EXTERNAL RELEASE WITHOUT APPROVAL BY [REDACTED] THREAT INTELLIGENCE



## Other

Any other cyber event or evidence of [REDACTED] network compromise deemed worthy of reporting that does not fall into the above categories.

**TLP: WHITE**

**CONFIDENTIAL: NOT FOR EXTERNAL RELEASE WITHOUT APPROVAL BY DOMINION ENERGY THREAT INTELLIGENCE**

Threat Response and Analysis Center  
[REDACTED]

## Document 6

# Identifying Unusual Behavioral Utility A

Guide for identifying suspicious or unusual behavior in the workplace

[Click here to return to the Table of Contents](#)

# Identifying Unusual Behavior

## Overview

Some high profile incidents have brought many security issues to the forefront of management concern. Reception personnel or anyone that has to deal with the public as the “face” of a company provide the first line of security for a location, and it is the intention with this information to provide personnel that interact with people from outside of their location with some knowledge that they require to safely perform their duties.

As a general rule, all persons approaching the reception area will be much easier to deal with if you start by making eye contact, smiling and begin the conversation with an appropriate ‘seasonal’ greeting. Remember, no one likes to be ignored. All visitors should sign in and out, and be escorted by the person they are visiting.

## Identifying Unusual Behavior

It is important that you develop a sense of what is normal behavior exhibited by persons arriving in your location. You should ‘benchmark’ normal arrival routines and compare new arrivals’ behavior against your ‘benchmark’. Most individuals visiting your location for the first time will pause briefly in the doorway, look for the reception area and then walk towards it, or they will walk directly to the desk without pausing. Visitors who are confused, or who have arrived early for an appointment, will normally approach the desk after eye contact has been made with him or her. People who do not approach the desk after eye contact has been made should be kept under close observation.

- These individuals may be waiting for an opportunity to ‘tailgate’ (follow someone through an access control point) into the office.
- Watch to see if they are looking for security devices such as door-release switches, locks and cameras.
- Suspicious or potentially violent visitors may also spend time evaluating escape routes, looking for a hiding place, or searching for a ‘weapon of opportunity’

If their behavior is suspect, call for assistance.

It is expected that when visitors approach your desk you will be engaged in conversation for a brief period of time. This is acceptable to a point. If the discussion becomes unfriendly, focuses heavily on the ‘business’ or an employee(s), or certain controversial aspects of company operations, you must immediately end the conversation. If you cannot end the discussion after two or three attempts and the situation becomes threatening, call for assistance and **do not** grant anyone access into the office area until the problem has been resolved. However, NEVER place yourself in harms way to prevent action of a violent or armed individual(s). Personal safety is always of utmost concern. If you must allow access to someone, let him or her through and dial 911.

People will often loiter by your desk while waiting for an employee or admittance. You should politely direct them to have a seat while they wait. If they choose not to sit down, it may be because they are interested to see what is on your desk. Therefore, it is very important that proprietary information, indeed all company-related matters, be kept out of sight. Try to maintain a tidy work area. Keep confidential material in a file folder or a locked drawer when not in use. Individuals may also be trying to see what type of security devices you have, where they are located, and how they operate.



# Identifying Unusual Behavior

Observe where people sit once they have interacted with you. Most business persons will sit near a telephone, if they do not have one of their own, or pick-up reading materials such as a Company Brochure. Sitting by a window that offers an interesting view or direct sunlight is also a popular spot to wait. You should be aware of individuals who sit very close to entrance/emergency exit doors or who sit out of view of the reception desk. During inclement weather, watch for people who do not remove their coat, hat, gloves, if applicable, while they are waiting, especially if it is for a long period of time. If you get an uneasy feeling from some of these visitors, discreetly call for help and delay their entry.

## Angry People

During the course of your duties, you may occasionally encounter angry people. The following section is designed to help you understand the different levels of anger and to assist you in determining if the person is a real threat.

<b>Stage 1: Anxiety</b> Defined as a 'noticeable change in behavior, an involuntary reaction or response to something that happens'. Some external changes triggered by anxiety are:	<b>Stage 2: Verbal Aggression</b> In order not to injure him/herself, an angry person will attempt to 'win' through the use of words and/or body language. Some external changes to watch for are:	<b>Stage 3: Aggression/Assault/Imminent Danger</b> External changes to watch for are:
<ul style="list-style-type: none"><li>• A flushed face</li><li>• Body twitching</li><li>• The appearance veins</li><li>• Sweating</li><li>• Twitching lips</li><li>• Head down</li><li>• Minimal eye contact</li><li>• Pacing</li><li>• Shallow breathing</li><li>• A dry mouth</li><li>• Frowning or twitching eyebrows</li><li>• Little verbalization</li><li>• Excessive fidgeting with eyeglasses, rings, pen, etc.</li></ul> <b>Anxiety is triggered by:</b> <ul style="list-style-type: none"><li>• Frustration or anger</li><li>• The loss of control</li><li>• The receptionist's body language, tone or demeanor</li><li>• A third party</li><li>• Depression</li></ul>	<ul style="list-style-type: none"><li>• A red face</li><li>• Standing as tall as possible</li><li>• Lips tightly pursed</li><li>• Hand waving and finger pointing</li><li>• Clenched fists</li><li>• Direct, prolonged eye contact</li><li>• Deep and rapid breathing</li><li>• Person moves into your personal space (e.g., closer than three feet)</li><li>• Excessive salivation</li><li>• Belligerent</li><li>• Cursing and yelling</li><li>• Eyebrows frowning</li><li>• Fists pounding on your desk or on the walls, etc.</li><li>• Stamps feet or kicks nearby objects</li><li>• Head and shoulders are back</li><li>• Shoulders are square</li></ul>	<ul style="list-style-type: none"><li>• Face turns white</li><li>• All verbalization stops</li><li>• Lips tighten over the teeth</li><li>• Breaks eye contact and begins to focus on a 'target'</li><li>• Very deep and rapid breathing</li><li>• Forehead creases and eyebrows furrow</li><li>• Head is down</li><li>• The shoulders begin to shift</li><li>• Person changes their stance</li><li>• Bobbing or rocking</li><li>• No movement at all</li></ul>

# Identifying Unusual Behavior

<ul style="list-style-type: none"><li>• The feeling of being cornered</li></ul>		
---	--	--

When dealing with anxious people, give them proper space, correct eye contact and non-confrontational facial expressions or posture. Listen carefully and use supportive, verbal communication. Introduce yourself, use your first name, and try and use their first name as often as possible. Avoid using the word 'you' when talking to them. If you do not understand something they have said, ask them to repeat it clearly. Try and use the word 'we' (e.g., "We will be happy to assist you.").

## *Eye Communications*

Break eye contact when you speak, but maintain eye contact while the angry person is speaking. Messages you may receive from the angry person's eyes are:

- Pupil size getting smaller, this means the person is getting angrier
- Person sizing you up
- Eyes jerking/darting
- Eyes looking around for possible access/escape routes, or for a 'weapon of opportunity'
- Eyes glazed, empty, or looking through you
- Eyes widening in fear
- Eyes glistening, ready to cry
- Eyes continually glancing at a target

## *Your 'Sixth' Sense*

The most important safety asset we have is our 'sixth' sense. Our five normal senses – sight, hearing, smell, taste and touch – combine to produce our 'sixth' sense. The 'sixth' sense is the ability of our subconscious mind to detect danger by responding to stimuli that our conscious mind may not be able to recognize or articulate.

Persons who can be exposed to potentially hazardous situations must be prepared to listen to their intuition or 'sixth' sense. Although it may not be apparent at the time, signals from the 'sixth' sense are always based on something (e.g., "That sports bag looks very heavy, or "That man is not making eye contact."). The 'sixth' sense picks up signals and analyzes them faster than we can do consciously. Intuition is a survival mechanism of the unconscious mind and as such, always has your best interest at heart. It will not tell you to put yourself in a dangerous situation.

Our 'sixth' sense speaks to us in many ways. Some of the warning signs of the 'sixth' sense are:

## *Physically*

- Acidic taste in the back of the mouth. This is caused by the 'fight' or 'flight' reflex sending blood from our vital organs to our arms and legs.
- Hair-raising on the back of the neck and arms
- Quavering voice

# Identifying Unusual Behavior

- Accelerated heartbeat
- Shallow, rapid breathing
- Feelings of fear, discomfort and/or panic
- Nagging feelings
- Resistant thoughts
- Humor (e.g., "I am leaving before that bomb goes off.")
- Wonder (e.g., "I wonder what is on his mind?")
- Anxiety Curiosity (e.g., "What is in that bag? It looks really heavy!")
- Hesitation
- Suspicion
- Apprehension
- Fear

# Document 7

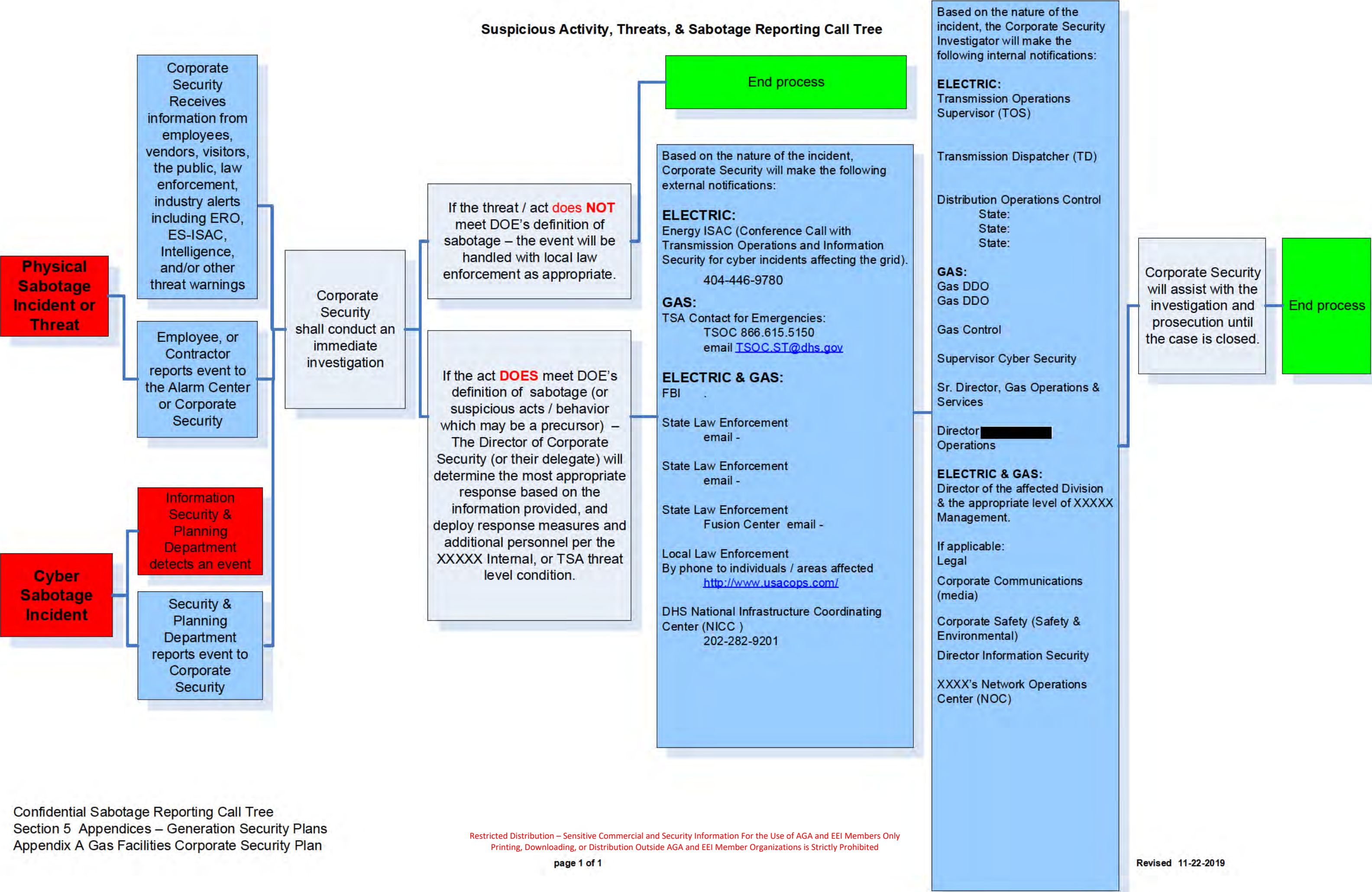
## Susp Activity, Threat and Sabotage Reporting

A process flow chart that illustrates the reporting process, key contacts, and response activities

[Click here to return to the Table of Contents](#)



Suspicious Activity, Threats, & Sabotage Reporting Call Tree



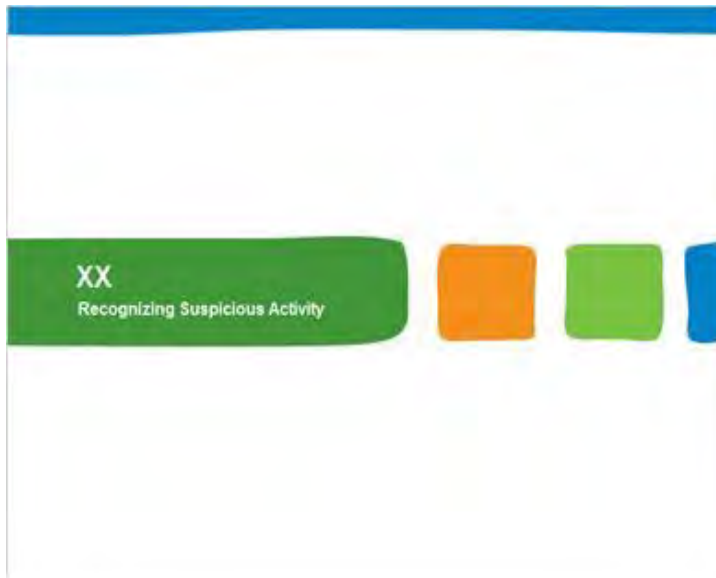
# Document 8

## Susp Activity Recognition CBT Utility A

Training slides for field employees on how to identify suspicious behavior

[Click here to return to the Table of Contents](#)

## 1.1 Reporting Suspicious Activity



## 1.2 CBT Instructions





## 1.3 Course Completion

### Course Completion

To receive credit for this course, you must take the quiz at the end of the CBT and score at least 80%.

## 1.4 Purpose

### Purpose

XX facilities may be attractive targets for intentional damage or interruption of service.

Attacks may consist of damage to a single XX facility or a coordinated attack on multiple XX facilities.

Any individual or group with the capability and intent to do harm could put XX at risk. This includes dissatisfied individuals, domestic and international organized aggressors, aggressor nations.

In addition, threats may originate from disgruntled employees who possess insider knowledge of the systems and equipment used in our facilities.



As an XX employee or contractor, it is your responsibility to be knowledgeable in observing and reporting suspicious behavior.



## 1.5 Purpose - continued

### Purpose - continued

In targeting XX, potential aggressors can employ a wide range of methods, including, but not limited to cyber attacks; disruption of fuel, electric and/or natural gas transportation or distribution, disruption of coal, gas and/or water transportation, and attacks on assets using firearms, explosives or other types of weapons.

Therefore, it is critical that we are aware of the possible threats, observant in the protection of our infrastructure, and prepared to act when threat indicators are present.



This course provides an understanding of the types of activities that can be considered suspicious and should be reported.

## 1.6 Objective

### Objective

The objective of the training is to provide you with information on suspicious activity recognition.

By the end of the course, you will:

- Recognize when XX is a possible target of an attack.
- Know who to contact when suspicious activity is observed.
- Identify potential indicators of threat activities.
- Detect surveillance methods.
- Recognize internal and external threats.

## 1.7 Who to Contact

### Who to Contact



#### Checklist

- ☐ **Personal Safety**  
If you feel personally threatened, leave the area immediately and call 911 or local law enforcement.
- ☐ **Facility and/or Infrastructure Protection**  
Call 911 or local law enforcement if the threat is imminent.
- ☐ **Known or Suspected Suspicious Behavior or an Incident of Intentional Damage or Intent to Damage**  
Immediately contact the XX Alarm Center  
: 

Upon notification, XX's Corporate Security will investigate all reports and take appropriate action.

## 1.8 Potential Aggressors

### Potential Aggressors

A potential aggressor is an individual or a group who possesses the capability and intent to do harm.

Potential aggressors include:

- Dissatisfied individuals or groups
- Disgruntled employees
- Organized adversarial groups
- Domestic and international terrorists
- Aggressor nations
- Participants of domestic violence and/or stalking situations

## ***1.9 Objectives of Potential Aggressors***

### Objectives of Potential Aggressors

#### Common Objectives of an Aggressor

- Intentional damage, disruption and/or casualties
- Obtain classified/confidential insider information
- Tarnish XX's corporate image and reputation
- Provide notoriety that some aggressors seek



## ***1.10 Aggressor Objective - Intentional Damage to a Facility***

### Aggressor Objective - Intentional Damage to a Facility

#### Damage or Destruction of a Facility Could

- Impact the operability of XX's bulk electric system and/or gas operations
- Compromise the structural integrity of XX's facilities
- Inflict casualties onsite



## 1.11 Aggressor Objective - Obtain Operational Information

### Aggressor Objective - Obtain Operational Information

Theft or Loss of Information or Equipment Could Pose a Risk to XX and/or the National Power Grid

#### Materials or equipment

- XX or contractor clothing, ID badges, keys, and/or vehicles could be used by an aggressor for unauthorized access to XX facilities or other non XX targets.

#### Operational information

- Information stored on XX electronic devices (laptops, phones, iPads, external storage devices, etc.), poses a risk to XX if not properly secured, or are left unattended.
- Hard copy schedules, plans, engineering drawings, sensitive emails, procedures, etc. pose a risk if left unattended on a desk, printer, vehicle or other location.

## 1.12 Aggressor Surveillance - Planning

### Aggressor Surveillance - Planning

The easiest time to detect an aggressor is during their surveillance phase.

- Aggressors use surveillance to identify and plan their attacks. Typically, the surveillance is conducted over an extended period of time in order to identify and plan the best means to attack the target.
- Recognizing and reporting suspicious behavior is our most preventive means of stopping aggressor attacks.
- Due to the fact that many of XX's facilities are remote, it may be more difficult for XX employees, civilians, and law enforcement officials to detect aggressor surveillance activities.





### ***1.13 Process of Planning an Attack***

#### **Process of Planning an Attack**

- Aggressors may use publicly available information to gather intelligence about the facility, such as building plans, Google Earth, etc. They may also attempt social phishing and ask suspicious questions of employees regarding security and procedures.
- Surveil a target facility for long or short period of time, possibly using advance electronic technology.
- Attack planning may include dry run attacks to test facility and test employee response.
- Conduct final surveillance to see if security and procedures have changed since the dry run attack.



### ***1.14 Surveillance Objectives***

#### **Surveillance Objective**

##### **Overall Objectives of Surveillance Activity**

- Identify targets
- Find weak points
- Determine the likelihood of success of an attack



## 1.15 Physical Security

### Physical Security



- Presence or absence of security cameras
- Number, location, type and coverage of security cameras
- Security screening procedures for employees, visitors and vehicles
- Restricted access procedures
- Proximity to first-responder locations
- First Responder response times
- Number, location, dress, weapons, and equipment of private and police security coverage

## 1.16 Facility Access Procedures

### Facility Access Procedures

Aggressors may assess:

- Size and location of staff
- Visitor access procedures
- Availability of tours
- Location of roadways, entrances and parking lots
- Delivery procedures - gate access (ingress and egress) in relation to the target




## 1.17 Physical Facility Layout

### Physical Facility Layout

Aggressors may assess:

- Construction materials used
- Building shape, height and setbacks
- Location of vulnerable structural components
- Opportunities for cascading damage effects to adjacent facilities or other infrastructure or customers
- Location of executive offices and employee meeting places
- Adequacy of emergency exits, escape routes, and fire suppression systems



## 1.18 Facility Operations

### Facility Operations

Aggressors may observe:

- Starting and ending work times
- Lunch and break times
- Shift changes
- Patterns of concentration of people and vehicles and traffic congestion
- Nearby people and vehicle movement throughout the day
- Police and security radio frequencies and recording of emergency response times
- Inspection times and frequency



## 1.19 Secondary Targets

### Secondary Targets

Aggressors may use secondary targets near an XX facility

- Nearby alternative targets (switchyard)
- Nearby collateral targets (water intakes, disrupting critical deliveries)
- Interruption of fuel delivery



## 1.20 Surveillance Positions

### Surveillance Positions

Surveillance positions are general areas used to perform surveillance on the facility's vulnerabilities, avenues of approach or may consist of activities that may aid in the planning or carrying out of an attack.

- Surveillance positions provide cover or concealment which can be used to perform covert surveillance.
- The surveillance position for a particular facility may change over time. For example, different times of day provide different lighting conditions, and changes of seasons may affect visibility from certain vantage points.



## 1.21 Counter Surveillance Positions

### Counter Surveillance Positions

- When identifying surveillance positions, consider that potential aggressors may need:
  - a view of their target.
  - safe entry to and from the area providing that view
  - a cover story
- They need to remain unseen or unnoticed, either by concealing themselves from view or hiding in plain sight, by disguising their purpose.
- Once an area has been identified to be the most likely surveillance point, surveillance detection efforts can be focused on where they will be most effective.

## 1.22 Sabotage Awareness

### Sabotage Awareness

It is the responsibility of every employee, contractor and service vendor to **IMMEDIATELY REPORT damage, destruction, physical threats and sabotage events to an XX facility that may include:**

- Tampering with or vandalism of infrastructure of electric grid components or gas distribution transmission systems, such as transmission towers, poles, transformers, substation equipment, telecommunications, etc.
- Disrupting the fuel or water supply to a power generation plant or disrupting operations by false, or substantiated threats (bomb, fire, biological hazard, etc.)
- Unexplained unlocked substation gates, doors, yard-cabinets, control houses or gas valves.
- Displaced manhole lids or control cable covers
- Unauthorized people requesting sensitive information (through emails, phone calls) about security systems, operations, software, facility staffing, telecommunications, etc.

#### Responsibility

A duty or obligation upon one (morally, or legal accountability) to behave correctly in respect of ability or authority to act or dec. take decisions independently.

## 1.23 Sabotage Awareness - continued

### Sabotage Awareness - continued

It is the responsibility of every employee, contractor and service vendor to **IMMEDIATELY REPORT damage, destruction, physical threats and sabotage events to an XX facility that may include:**

- Unauthorized people plugging devices into the data or telecommunications network, unauthorized downloading of materials (e.g., maps, photographs, schematics or similar materials) that could be used in conjunction with surveillance or attack-planning activities
- Verbal or written threats targeting security systems, software, operations, or facilities
- Suspicious packages located at XX facilities
- New or unauthorized equipment in the vicinity of the cyber assets
- Workstations or laptops that start working in uncharacteristic manner

#### Responsibility

A duty or obligation upon one's moral, or legal accountability in respect or to behave correctly in respect or ability or authority to act or decide take decisions independently.

## 1.24 Suspicious Behaviors

### Suspicious Behaviors




- Unauthorized individuals using or carrying video/camera/observation equipment.
- Unauthorized individuals with installation maps, photographs or diagrams with highlighted area, notes regarding infrastructure or a listing of installation personnel.
- Individuals possessing or observed using night-vision devices near the facility perimeter or in the local area
- Individuals parking, standing or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
- Facility personnel willfully associated with suspicious individuals.

## 1.25 Performance Changes

### Performance Changes

Anyone Who Radically Changes Work Behavior

- Unexpectedly changes working behavior or requests to work irregular hours without a valid reason
- Increased absenteeism or on-the-job absenteeism
- Difficulties in concentration/confusion
- Lowered job quality/efficiency
- Sporadic work patterns
- Increased accidents
- Diminished interpersonal skills

An analog clock with a black face and white numbers, showing the time as approximately 10:10.

## 1.26 Behavior Changes

### Behavior Changes

Anyone Who Radically Changes Personal Behavior, Appearance or Habits

- Extreme behavior
- Unusual interest in violence or conflict
- Comments about getting even or acts of violence
- Overt threats of violence
- Excessive talk about weapons (not hunting or target/trap shooting enthusiast discussions)
- Noticeable withdrawal
- Noticeable decrease in communication
- Unusual appearance of calm or detachment

Two brass bullets, one slightly behind the other, both pointing towards the right.

## 1.27 Signs of Attack

### Signs of Attack

#### What To Look For:

- Inappropriate clothing for the season
- Excessive behaviors (fidgeting, clock watching, area scanning)
- Rigid posture with minimal body movement or arms close to sides
- Appearing to be in disguise
- Drastic and sudden change of appearance (shaved body hair, shaved head, increased mass from explosive vest)
- Unauthorized individuals in possession of uniforms or identification badges
- Discover breaches in physical security (security camera or phone lines cut)
- Delivery of equipment or material that is suspicious, unexpected, unusual, out of the norm, without explanation or with missing paperwork
- A seemingly abandoned or illegally parked vehicle in the area of the facility of asset

## 1.28 Reporting - Your Responsibilities

### Reporting - Your Responsibilities



- ☐ **Personal Safety**  
if you feel personally threatened, leave the area immediately and call 911 or local law enforcement.
- ☐ **Facility and/or Infrastructure Protection**  
Call 911 or local law enforcement if the threat is imminent.
- ☐ **Call the XX Alarm Center**





## 1.29 Reporting - Your Responsibilities

### Reporting - Your Responsibilities

#### Checklist

- ☐ Unless absolutely necessary for safety, DO NOT touch, walk through or disturb any type of evidence, until the proper authorities have arrived on scene to investigate
- ☐ Take notes - document WHO, WHAT, WHERE, WHEN, WHY and HOW
- ☐ When possible, take photographs
- ☐ Follow your departmental plans and procedures, if any, for responding to such incidents or events

## 1.30 Time for Quiz

### Time for the Quiz

To receive credit for this course, you must score at least 80%.

Do **not** close the course by using the window's X button.

The **EXIT** button at the top of the screen allows you to exit the course. But remember, do not click **EXIT** before completing the course or you will not receive credit for the course.