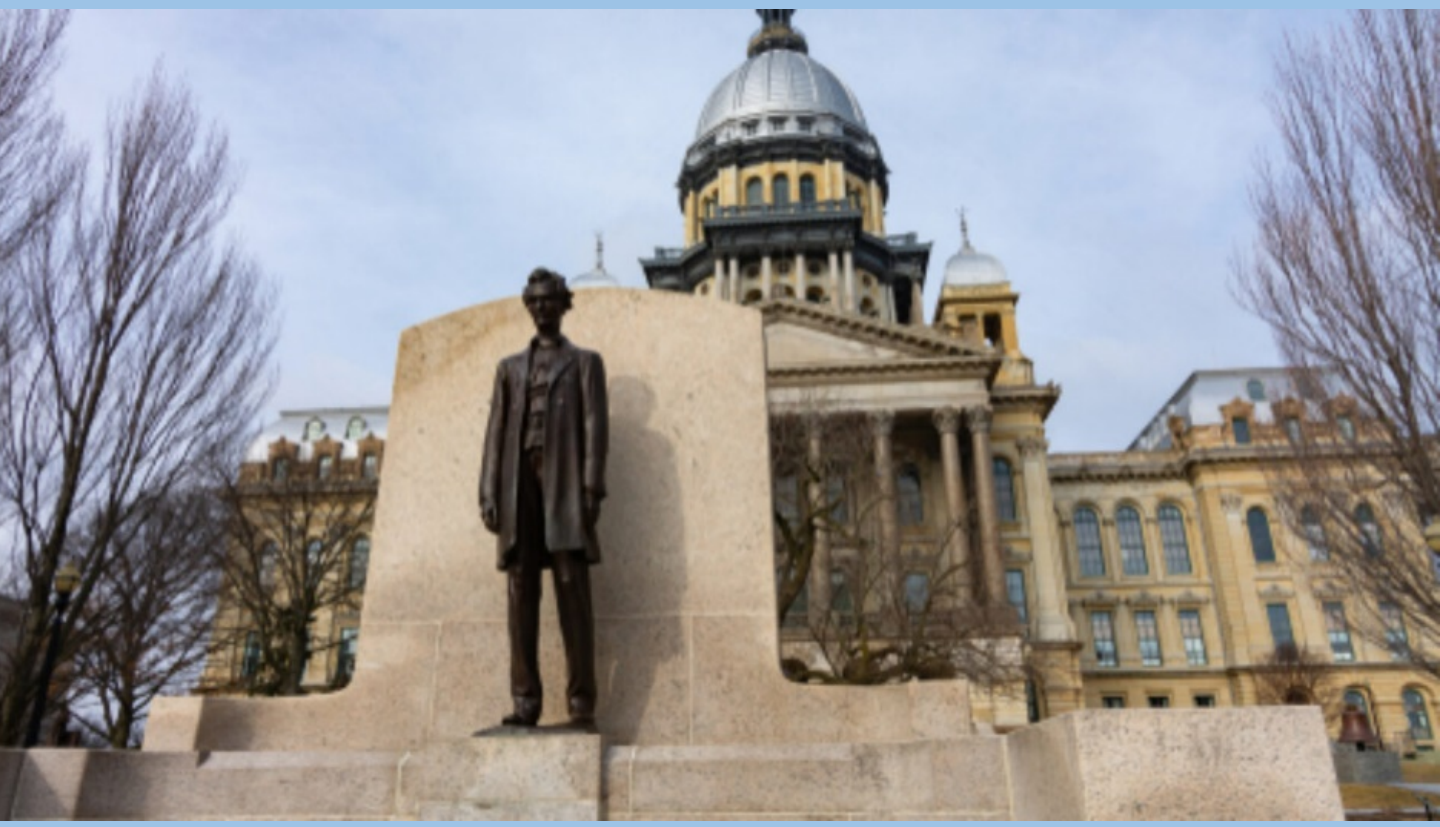
Communicated Threat Recognition and Management Guide

for State of Illinois Agencies



Prepared by
Illinois State Police
July 2023

This Page Intentionally Blank

ILLINOIS STATE POLICE
Office of the Director

JB Pritzker
Governor

Brendan F. Kelly
Director

July 30, 2023

To State of Illinois Agency Leaders:

It is a primary mission of the Illinois State Police (ISP) to promote public safety through enforcement, education, and especially through cooperation with all of our partner agencies in the State. To assist in this effort, the ISP has prepared this guide for you and your agency as a reference for recognizing, reporting, and managing threats. These threats, also known as Inappropriate Contacts and Communications (IC&C), take many forms, and accurate recognition and awareness of the resources and mechanisms available for reporting them is the best mitigation.

This Guide refers to other references, such as an *Emergency Action Plan* (EAP) template provided by Illinois Department Central Management Services, and a Continuity of Operations Plan (COOP) template provided by the Illinois Emergency Management and Homeland Security Agency. Additionally, there is a guidebook available from the ISP titled "*Physical Security Considerations for State of Illinois Assets*," which is a comprehensive guide for securing your agency's assets. There are also individual, digital copies of worksheets, including a "*Communicated Threat Worksheet*," and informational flyers for suspicion indicators, suspicious packages, and techniques for diffusing aggressive behavior. These documents and links are available on the ISP website on the "Office of the Director" page, under the tab "Resources for State Agencies."

Finally, a training opportunity is available on the One-Net Training platform entitled "*Civilian Response to Active Threat*." Your One-Net training coordinator has the ability to add this program to your agency's mandatory training list for employees. I encourage your agency to take advantage of all of these valuable tools.

The Illinois State Police remains your partner and resource in providing a safe working environment for all State Employees.

Respectfully,

B F Kelly

Brendan F. Kelly
Director

801 South Seventh Street • Suite 1100-S
Springfield, IL 62703-2487
(217) 782-7263 (voice) • 1 (800) 255-3323 (TDD)
www.illinois.gov • www.isp.illinois.gov

This Page Intentionally Blank

Introduction

This Guide is designed to provide State employees and stakeholders with a process for recognizing, evaluating, and reporting Inappropriate Contacts and Communications. It is suggested that you read it in its entirety when you first receive it, and then periodically review it (once a month, for example). Just like a parachute, it is a best practice to have awareness of the concepts in this guide *before* you need to use it, rather than reading through and trying to learn the material *on the fly*.

IF YOU OR OTHER PEOPLE IN YOUR WORKPLACE ARE IN IMMINENT THREAT OF PHYSICAL HARM, IMMEDIATELY ATTEMPT TO LEAVE THE AREA AND CONTACT LOCAL LAW ENFORCEMENT BY CALLING "911" OR OTHER MEANS. FOLLOW YOUR EMERGENCY ACTION PLAN.

What is an Inappropriate Contact and Communication (IC&C)?

In the course of your official duties every day, you will likely come into contact or communicate with a variety of people. They may be the general public, clients or other consumers of state services, vendors, or even co-workers. These interactions are generally professional, but they may occasionally involve some degree of conflict, from mere disagreement, to aggressive behavior, to a physical altercation. In some cases, you may receive a phone call, an email, or a letter that contains language that is rambling, unsettling, or even outright threatening.

The term used by law enforcement to describe these various interactions is "*Inappropriate Contacts and Communications*," or **IC&C**. While every communicated threat is an IC&C, not every IC&C is a threat. This Guide is designed to give you the tools to recognize a potential IC&C, conduct a preliminary evaluation, and properly report the situation, when appropriate, to law enforcement.

Before we start, understanding a few important concepts is in order. Citizens have a *constitutional right* under the First Amendment to "petition their Government for redress of their grievances."[1] Clients and other consumers of government services generally communicate appropriately, but sometimes they may be rude, crass, or even outright hostile. The best way to work with these types of individuals is to practice good customer service and use appropriate diffusing and refocusing techniques (examples of various diffusing techniques are identified below).

Occasionally, individuals may engage in threatening behavior. A ***Threat*** is an expression, by any means of communication (written, verbal, electronic, body language, etc.), of the intention to inflict or cause some type of physical harm (including death) against a person, group, building, or other entity. Please note that a threat to "*expose*

[1] First Amendment to the U.S. Constitution: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"

corruption," report the state employee to the media or "*the authorities,*" to "*take legal action,*" or harm their political career are generally not considered threats for purposes of law enforcement. This guide specifically refers to threatened acts of ***Targeted Violence*****,** which refers to situations in which an identified (or identifiable) perpetrator "poses (or may pose) a threat of ***violence*** to a particular individual or group."

Generally, threats are NOT constitutionally protected, but one additional factor when evaluating an IC&C should be considered, and that is the concept of a "True Threat" vs. Hyperbole (also known as "Venting"). The courts have developed several views of assessing communications that are considered to be "threats." For purposes of this guide, you are not expected to analyze each and every IC&C for the legal nuances of a threat, but it is helpful to understand that clients may be frustrated while accessing your services, and may lash out in their communications. When appropriate, you should attempt to diffuse and refocus them. In many cases, they will acknowledge that they were "venting" and did not mean to be threatening.

Types of Threats:

Threats may fall into one or more general categories: *Direct*, *Veiled* and *Conditional*. It is significant to remember that a clear *statement of intent* is not always necessary to show the potential for Targeted Violence. It is important to always consider context and behaviors associated with the communication when recognizing and evaluating whether a communication is a threat. Examples of the various types of threats are described below.

A Direct Threat is usually pretty clear. For example "I will kill you," or "I'm coming down there to beat you up," or "there is a bomb that is going to explode there, get out." A direct threat is usually clear and unambiguous. While the intent and capability to carry out the threat are important factors in the law enforcement analysis of a threat, many times a Direct Threat may constitute a crime in and of itself. This will be discussed further below.

Another type of threat is a Veiled Threat. These types of threats may sound subtle, like "Bad things could happen to you," "the office might get shot up," or "somebody ought to straighten you out." Other factors such as tone and context are very significant, especially when it is not a direct statement. Some individuals may have the intent to threaten but want plausible deniability if they are challenged later. If you are the recipient of this type of communication, it is important to form an opinion as to the effect it has on you based on what you are hearing and the way it is conveyed.

The final type of threat is a Conditional Threat. Just as the term implies, the intent is for the target of the threat to do, or not do, something in their control or face consequences. Examples would include "if you don't void that ticket, I will hurt you," "if you vote yes on this rule, I will hunt you down," or "issue my benefits, or you will get hurt." In some cases, a conditional threat may be paired with a veiled threat. For example, "if you don't issue my refund, bad things could happen."

Subjects who Make IC&C:

IC&C are as diverse as the persons who make them and must be appropriately evaluated, but the good news is that the majority of IC&C do not indicate a threat. As discussed above, those who make IC&C include general citizens, clients and consumers of your services, vendors, and even other state workers. Identification of the subject, when possible, is an important component of appropriately assessing an IC&C. Understanding the individual and their motivation goes a long way to understanding the IC&C in context and evaluating whether it conveys a threat. Occasionally, you may receive an anonymous IC&C, and while some information may be missing, it will be evaluated in the much the same way.

IC&C can be delivered in many ways. They may be mailed in through the U.S. Postal Service, delivered by messenger, left as a note or writing on something on-site, emailed, texted, social media, otherwise posted on-line, via telephone, and obviously in person. Additionally, it may be conveyed by a third party, perhaps as an overheard conversation. Just as understanding the subject making the IC&C is an important

component of the evaluation process, knowing the delivery method is also important in the evaluation process, especially when it is anonymous.

Additionally, the target of the IC&C is a relevant factor. For example, the target spectrum may include a specific individual, a representative individual (e.g. the Director, the Bureau Chief, etc.), a particular facility (e.g. the local service office, the hospital, etc.), an institution (a school, the Department of Revenue, the Court etc.) or even the Government itself. The process of evaluating an IC&C is generally the same across the spectrum, but each type of target may involve some special criteria. For example, the threat of school violence and threats against Government leaders will take additional factors into consideration as they are evaluated.

Finally, the methods used to preserve an IC&C for follow–up investigation and future prosecution, if appropriate, will depend on how it is delivered. For example, a text, voice mail, video, or email IC&C will require digital methods to document and preserve the content, whereas notes and packages delivered by mail/messenger, in person, or left on-site will require different physical preservation. Specific methods of preservation based on the type of IC&C will be discussed below.

The Process for Recognizing, Gathering Information, and Evaluating an IC&C:

Receiving a threat may be disturbing; but if you keep a few things in mind, you can deal with the apprehension of a threat. First, the value of a threat is whatever value the recipient gives to the threat. In other words, respect the threat, but do not allow it to overly affect you. Second, threats are usually not made from a position of power and are intended to intimidate whether or not the maker of the threat can or intends to carry out the threat. With that understanding, how do we identify an IC&C?

Any communication or contact that makes you feel uneasy, including Direct, Veiled or Conditional Threats. Additionally, an IC&C may include, but is not limited to, content and circumstances involving:

- The presence of indicators identified in the Suspicious Package Protocol
- Obsessive interest in the target, including a desire to meet
- Obsessive references to perceived grievances (valid or otherwise)
- The substance and form of the writing
- Bizarre and disorganized thoughts and behaviors
- A history of prior inappropriate behavior
- Improper surveillance or stalking behaviors
- Continuous or routine harassment by phone or otherwise
- Other behaviors of concern
- References to violent incidents (mass shootings, etc.)

While an IC&C may make you feel generally uncomfortable, learning to articulate the specific issues in terms of content and context will improve the evaluation process and its outcomes. In other words, it is okay to have a hunch, but the better you can describe why you have that hunch, the better the process will be. Finally, it is important to note that even though an individual engages in harassing or other IC&C type behavior (short of threats), we still have a duty to provide professional service until an official disposition is made in the matter.

A worksheet is available to help organize the process of information gathering related to the IC&C. The "*Communicated Threat Worksheet*" is available for download through the Illinois State Police website under the "Office of the Director" tab, in the "Resources for other State Agencies" section. The goal of this worksheet is to capture as much information as possible regarding the substance, maker, delivery, and context of the IC&C.

Preserving the IC&C:

While most IC&C will not result in criminal charges, some may become evidence in a criminal prosecution or even an administrative proceeding against the sender. Because it may not be immediately apparent which direction an IC&C will take, we need to properly preserve each IC&C as if it will be used as evidence. Evidence may take many forms, including but not limited to: Written letters and notes, graffiti, in-person statements, electronic messages and recordings, etc. The term for this process is called maintaining the "*chain of custody.*" Below is general guidance for preserving chain of custody, but be aware that law enforcement may require additional actions, such as completed receipts and gathering "elimination finger prints" of everyone who handled the object. Common sense is always appropriate in dealing with preservation issues.

If the IC&C is delivered in person:

- Attempt to disengage, then contact 911 if you are in fear for your safety
- Give the best description of the individual possible, including name and contact information (if available), vehicle information and the direction of flight
- If the IC&C is simply bizarre or otherwise inappropriate and you are not in fear for your safety, gather information and report it to your supervisor as soon as possible
- If there is video footage capturing the interaction, it will need to be preserved

If you discover a suspicious package:

- Follow the Suspicious Package protocol below

If the IC&C is delivered as mail, a note or a package, and is not overtly suspicious:

- Preserve the item (a large envelope, paper bag or plastic sleeve is appropriate)
- Limit handling, and identify all persons that have handled the item
- Contact your supervisor for notification and guidance as soon as it is safe to do so

If the IC&C is delivered by phone:

- Try to capture the number on caller ID, if available
- Utilize the Communicated Threat Worksheet to capture relevant information, especially voice features and specific language used
- If indicated, follow bomb threat protocols, as described below
- Contact your supervisor and local law enforcement for notification and guidance as soon as it is safe to do so
- If the caller is a chronic harasser, advise them that their calls are harassment, and document that you have told them. (In accordance with 720 ILCS 135/1-3)

If a message is left on Voice Mail:

- Save the message in the voice mail system and do not erase it
- Report the situation to your supervisor

If the IC&C is delivered by email, via a social networking site, or otherwise on-line:

- Do not erase it or close the application
- Contact your supervisor for notification and guidance as soon as it is safe to do so
- Steps taken to preserve the document may include saving the message, taking a screen shot of the message or application, printing it or other means (Each application is different, and may require special steps to preserve the message)
- Additionally, if the delivery is via a social media platform, contact the provider(s) to advise the nature of the IC&C and request that they preserve the communication for law enforcement.

If you become aware of an IC&C directed at another person:

- Attempt to locate and advise the target(s) of the IC&C
- Report the incident to your supervisor providing as much information as possible

If you get an order of protection through the courts (related to on or off-duty issues):

- Advise your supervisor and provide a copy
- Include as restricted locations in the document your location of work assignment, and include all related space (i.e. parking lot, etc.) and any satellite locations you may be assigned to work
- Keep a copy of the Order of Protection on your person and in your vehicle

Reporting an IC&C:

IF YOU OR OTHER PEOPLE IN YOUR WORKPLACE ARE IN IMMINENT THREAT OF PHYSICAL HARM, IMMEDIATELY ATTEMPT TO LEAVE THE AREA AND CONTACT LOCAL LAW ENFORCMENT BY CALLING "911" OR OTHER MEANS. FOLLOW YOUR EMERGENCY ACTION PLAN.

Once it is determined that an IC&C should be assessed at a higher level because it may convey a threat, your supervisor should coordinate the appropriate notifications, in accordance with the local facility EAP. A suggested process would include:

- Complete the "*Communicated Threat Worksheet*" as soon as it is safe to do so
- Contact your Local law enforcement Agency (and fire/ambulance, if appropriate) in accordance with your emergency action plan
- Follow the response and preservation guidance provided in this document
- Be prepared to cooperate with first responders and investigative personnel
- When appropriate, activate your established internal response protocol

Of note, it is critical that the specific individual, or individuals who received the IC&C are available to answer follow-up questions in a timely manner. *There are many documented cases of a miscommunication or a misunderstanding leading to an unwarranted threat response*, which leads to a waste of resources and potential constitutional violations. If the individual cannot remain physically, they should provide a cell number or other means of direct contact.

Managing the Situation:

As described above the response to an IC&C, whether it is a verified threat or an otherwise concerning contact or communication, is a process. After the initial response is conducted, there are additional appropriate actions an agency can take to promote a safe environment. In addition to criminal investigation and prosecution in cases that warrant that response, the Agency can do any combination of the following:

- Establish a multi-disciplinary committee to handle these situations. Participation may include your internal legal, HR, security, operations, and executive level personnel
- Provide notice to the individual that their communication was harassing, concerning, or otherwise inappropriate and request that they refrain from that behavior
- Take appropriate administrative action against the client or employee (e.g. discipline or other sanctions)
- For employees, consider a corrective action plan in consultation with your legal and HR division
- Court ordered interventions
- Take steps to limit physical access or provide alternate mechanisms for access to Government services (this would generally require notice to the individual)
- Identify an “Ombudsman” point of contact and limit agency communications to that individual point of contact
- Without rewarding bad behavior, review the client’s case and see if appropriate services can be provided to close the matter

The above is not an exhaustive list, but rather examples of past actions and interventions that have produced successful outcomes. Remember that repeated IC&C, or failure to abide by the above strategies may indicate that the situation should be reviewed for escalated threat assessment.

Other Notifications:

Generally, law enforcement notifications regarding IC&C of concern should be directed at your local law enforcement agency, whether it is the local police department or the county sheriff's office, as appropriate to your area and identified in your facility EAP. They are your designated first responder, and this ensures that they are aware of the situation, especially if it is an emergency or exigent situation. In many cases, that agency will follow up with the Illinois State Police as part of their investigative process if it is warranted. Failure to follow the below process could result in delays and miscommunication.

If your agency management decides the matter should also be reported directly to the Illinois State Police, the following procedure *must be followed*:

The following information will be submitted by an *ISP designated Security Liaison from your agency* in the appropriate format:

- The name of the local investigating agency, their case number and a direct point of contact (e.g. Det. Smith or Officer Jones) with their phone number and an email address
- The name of a management direct point of contact for your agency along with a phone number and email address
- A completed copy of the *Communicated Threat Worksheet* for this matter
- A general narrative of the event and why it is being directly reported to the ISP

In addition, gather any other information you have on the subject (for example, their case file, past history of service, current contact information, etc.) and have it available to the management point of contact for discussion.

In conclusion, the Illinois State Police is committed to promoting a safe work environment for all State of Illinois employees and the public they serve. This guidebook will assist your agency and work unit in preparing for and dealing with an IC&C event. For additional information, and to access various resources related to IC&C and Physical Security visit the "Resources of other State Agencies" page of the Illinois State Police website at "https://isp.illinois.gov/Director/ResourcesForOtherStateAgencies"

COMMUNICATED THREAT WORKSHEET

State of Illinois

Incident Date: _____ **Time:** _____

Type of Threat: ☐ **Targeted Physical Violence** ☐ **Shooting** ☐ **Bomb/Arson** ☐ **Chemical** ☐ **Other**

Received VIA:

☐ **Phone - Receiving #?** _____ **Caller ID?** _____

☐ **Text: Screen-shot the Texts, do not erase or forward text until directed to do so**

☐ **E-Mail: Do not erase or forward email until directed to do so**

☐ **Letter/Package: Follow the Suspicious Package Protocol identified in the *Communicated Threat Recognition and Management Guide* or your facility's EAP**

☐ **Note left on-site: Do not handle the Note or writing, secure the area**

☐ **Other:** _____

☐ **In-Person: Provide all information, if known or estimated:**

Name: _____ **DOB / AGE:** _____

Address: _____

Phone: _____ **Email:** _____

Height: _____ **Weight:** _____ **Hair:** _____ **Eyes:** _____ **Sex:** _____

Clothes: _____

Carried Items: _____

Vehicle: _____

Speech:

☐ **Slow** ☐ **Disguised** ☐ **Coughing**

☐ **Normal** ☐ **Slurred** ☐ **Accent**

☐ **Fast** ☐ **Nasally** ☐ **Rambling**

☐ **Exited** ☐ **Aggressive** ☐ **Stuffy**

Background Noise: _____

_____

Other _____

_____

_____

***Person directly receiving or experiencing the incident*:** _____

Cell Number: _____ **Email:** _____

< OVER >

COMMUNICATED THREAT WORKSHEET

State of Illinois (Continued)

<u>QUESTIONS TO ASK</u>: (Ask as many as you can, even if they don't give you an answer)

Why are you doing this (what is the grievance)?

What is it you want/How can we help you?

That sounds threatening, is that a threat?

What do you plan to do? How will you do it? When/where will the attack take place?

<u>For Bomb threats</u>:

What kind of bomb is it?

When/how will it detonate?

Where is it? How did you put it there?

What does it look like?

WHAT WERE THE *<u>EXACT</u>* WORDS USED:

_____

_____

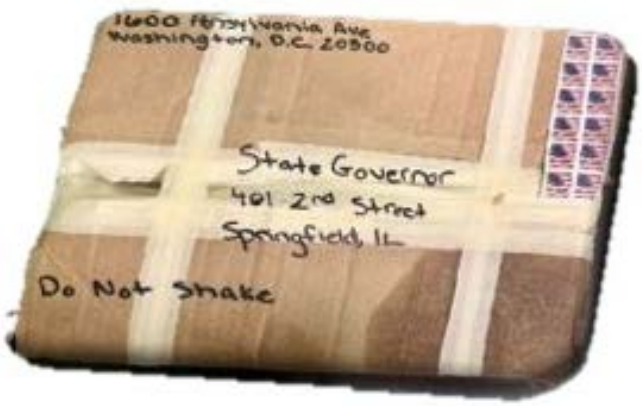
_____

_____

Suspicious Package or Letter Protocol

What makes a package (or Letter) suspicious? There are a number of observable indicators that might indicate the need for further inquiry. These characteristics may include, but are not limited to:

- The package is not expected or was un-solicited
- Excessive postage; non-cancelled postage
- Generic or incorrect title
- Unexpected weight of the package
- Lopsided and uneven
- Misspelled words
- Missing or unknown return address
- Nonsensical return address
- Oily stains
- Protruding wires
- Restrictive markings; handwritten notes
- Sealed with tape; excessive tape
- Unknown powder or substance



While one characteristic of suspicion may indicate a problem, you should look at the overall package or envelope before making a determination. If in doubt, activate the handling protocol, as described below:

- Remain calm and rational
- Do not touch, move, or open
- Notify your immediate supervisor and follow your Facility Emergency Action Plan (EAP)
- Stay in the immediate area unless explosives are detected or signs or symptoms of exposure develop
- If you suspect the item contains an explosive, evacuate the area and at least one floor above and one below
- Isolate the letter or package and close off the area
- If there is a powder or other discharge, secure the area and try to turn off the HVAC Air system
- Wash your hands with soap and water
- List all persons who touched or were otherwise in contact with the item
- Segregate exposed employees

For bomb threats that are received:

- Utilize the *Communicated Threat Worksheet* to capture relevant information
- Contact a supervisor and follow the notification procedures in your local facility EAP
- Have staff that is familiar with their area and common areas around them check for unusual packages, disturbed items, or other suspicious indications
- If a suspicious item is discovered, follow the above protocol
- Consider evacuation in accordance with your local facility EAP

If in doubt, contact a supervisor and activate your local facility EAP

Techniques for Diffusing Aggressive Behavior

"*If you can keep your head when all about you are losing theirs and blaming it on you . . .*" Rudyard Kipling

Sometimes people react to difficult or stressful situations by losing control of themselves, becoming loud and argumentative, irrational, and even being aggressive. So, how do you deal with this conflict? First, let's identify some indicators of aggressive behavior. Indicators of aggressive behavior, may include, but are not limited to:

- Increasing anxiety and irritability
- Escalating physical gestures (e.g. pointing, flexing, intimidating, etc.)
- Hyper-arousal (e.g. increase in respiration, skin reddening, etc.)
- Getting inceasingly louder
- Using disparaging, or condescending, "threatening" language

Trust your instincts regarding the behaviors exhibited and the need for additional assistance, when appropriate.

Concepts for Diffusion

- First and foremost, ensure your safety and the safety of your co-workers
- Position properly and have an exit strategy
- Make sure a co-worker or security officer is aware you are having an issue with the subject
- Know when it is time to end the conversation and withdraw
- Handle the situation directly and calmly
- Project confidence, balance assertiveness and empathy
- Be self-aware of your body language, posture, movements and tone
- Remain professional, do not let the subject "push your buttons" or goad you
- Utilize "Active Listening" techniques: Allow them an opportunity to be heard, reflect what they are saying and respond appropriately
- Don't be afraid to take a "time out" and allow some de-compression
- Identify the emotion (e.g. "you seem to be upset", or "you seem to be getting more frustrated") but NEVER say "relax" or "calm down"
- Try to "Re-Focus" the subject and get them to work with you to solve the problem, encouraging the subject to take responsibility for their own behavior and to direct it into more creative or positive outlets. For example, you might say:
    - "I'm trying to help you, but your anger is counter-productive. To solve this issue for you, I need you to work with me," or
    - "I need to check on this file, please give me a moment" and allow them time to de-compress and cool off

Suspicious Activity Indicators

You may observe activity around the facility or inside the workplace that you consider "suspicious." Generally, we look at *observable behaviors* to identify suspicious activity and do not rely on factors such as race, national origin, creed, or other innate factors. Being able to articulate the suspicious behaviors will help to better define why the behavior is suspicious.

It is important to note that many innocent behaviors may appear to be unusual or odd but do not pose a threat. While one particular action may strongly indicate suspicious behavior, we usually look for patterns or clusters to give a better indication of potential threat. For example, a person may simply be waiting for a friend and is looking at their cell phone to pass time, or perhaps they take a picture of an architectural feature. This in and of itself may be innocent behavior, but when you see a pattern of several Suspicion Indicators, it may be appropriate to make notification.

"Suspicion Indicators" might include, but are not limited to, the following examples:

- Active searching - Looking into parked vehicles, storage areas, loading dock areas, or appearing to conceal themselves in landscaping areas or when people walk by, appearing to "select a target," etc.
- Barred individuals loitering in the area – former or suspended employees, barred clients, individuals identified as making inappropriate contact or communications, etc. who are loitering in the area or repeatedly return after being instructed not to be on or near the premises.
- Elicitation – asking questions about security features or procedures, personal information, etc.
- Attempting to gain access to unauthorized areas – Acting "Lost" or like they belong in the area (but do not have the proper identification), attempting to by-pass locked areas, "talking their way in" to an unauthorized area, impersonating service providers, otherwise probing security, etc.
- Information Gathering – Loitering in an area for prolonged times or on multiple occasions with no discernable purpose other than to observe patterns of activities. For example, watching to see what times employees come and go, what doors they use, what vehicles they drive, taking notes that appear to be related to activities at the facility, observing evacuation routes and rally points related to fire alarms, etc.
- Photography – Taking pictures of features other than architectural attractions such as security screening areas, parking lots, entrance and exit doors, loading docks and other service areas, critical infrastructure, etc. especially if they are attempting to do it secretly or in an evasive manner.
- Suspicious Vehicles – occupied vehicles that appear to be conducting surveillance as identified above
- Multiple sightings over time and distance – Especially when it relates to a facility activity (e.g. end of the business day, truck deliveries, etc.)

If you observe articulable Suspicious Activity, notify a supervisor in accordance with your local Emergency Action Plan. If you believe that there is a potential for imminent criminal activity, immediately contact your local law enforcement. Utilize the "*Communicated Threat Worksheet*" to document information for law enforcement follow up.