NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.



U.S. Army Materiel Command (AMC) BLUE DART PROGRAM

for Major Subordinate Commands

09-1474-001 USAMC Blue Dart DG.indd 1 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

WHAT IS BLUE DART?

BLUE DART is a brevity code for the United States Northern Command (USNORTHCOM) emergency threat notification system. This handbook establishes procedures to direct and guide U.S. Army Materiel Command (AMC) installations, units, or activities in the execution of duties connected with the BLUE DART notification system.

SCOPE

BLUE DART provides emergency notification to installations, units, or activities within the USNORTHCOM Area of Responsibility (AOR) for whom USNORTHCOM has received a credible warning of an imminent attack. The system is designed to rapidly disseminate threat information and warn affected areas and units quickly (15 minutes voice) using a simple and easily understood format.

BLUE DART warnings are initiated by the USNORTHCOM NC-J3 through the USNORTHCOM Domestic Warning Center (DWC).

QuickStart

This handbook promulgates guidance, information, and procedures for use in the event of a BLUE DART notification. AMC Major Subordinate Commands (MSCs) will establish procedures to direct and guide installations, units, or activities in the execution of duties connected with the BLUE DART notification system.



COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

EXECUTION

To provide AMC installation commanders with the framework and guidance necessary for the development of their own local BLUE DART threat notification procedures that will be following references (A) through (E).

Concept of Operations

A. The USNORTHCOM DWC will issue a BLUE DART warning to affected installations, units, or activities when USNORTHCOM receives a credible warning of an attack that includes the following three elements of information regarding the threat:

1. A specific timing of the threat (normally within 72 hours)
2. A specific target (normally a specific unit, installation/ facility, or activity)
3. A specific means or method of attack is known (e.g., small arms, explosive device)

B. Initial notification is usually made via telephone (secure depending on availability). The initial notification will be followed by a "FLASH" precedence Operations Event Report-3 (OPREP-3) BLUE DART Message that will originate from the USNORTHCOM DWC.



COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Concept of Operations (Cont'd)

C. Any installation, unit, or activity located in the USNORTHCOM AOR that receives a credible threat warning from another source besides USNORTHCOM, must immediately report the information to the USNORTHCOM DWC at **719-554-9100**, followed by the release of an OPREP-3 Message with a "FLASH" precedence. Reference (B) provides detailed guidance and instructions regarding the preparation and release of an OPREP-3 Message.

QuickFlip

The chain of command must also be notified as soon as possible. See Steps 3 and 4 of Enclosure 3 in the "Enclosures and Formats" tab.

D. Installations, units, or activities that receive BLUE DART notifications must acknowledge receipt via telephone within 15 minutes, and AMC OPS Center via SIR Message within one hour. When acknowledging notifications via telephone, the installation, unit, or activity must use the known/verified USNORTHCOM DWC phone number (**719-554-9100**) to confirm that the notification is not a hoax. Enclosure (1) must be completed when receiving and acknowledging BLUE DART telephonic notifications. Enclosure (2) is a sample format for Naval Message acknowledgements. Acknowledgement messages must be submitted to the USNORTHCOM DWC as an attachment to an email. The email subject line must read "OPREP-3 SIR ACKNOWLEDGEMENT OF BLUE DART."

E. Upon completion of required BLUE DART voice reports and OPREP-3 Message release, installations will make entries to the Control, Communications, Computers, and Intelligence (C4I) Suite noting BLUE DART notification, responses, and follow-on actions.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Coordinating Instructions

A. AMC, HQ, and its component installations will ensure they are prepared to receive, disseminate locally, and acknowledge the receipt of a USNORTHCOM BLUE DART threat warning as detailed in this Order. This capability must be maintained at all times (24 hours a day, seven days a week, 365 days a year).

B. Once voice notifications are completed, affected installations will issue an OPREP-3 providing a detailed description and assessment of the threat and any actions that the installation has initiated in response to the warning. Affected installations will follow this OPREP-3 with supplemental reports in order to keep the chain of command abreast of the threat and installation measures to address the threat.

C. **Enclosure 1** contains a BLUE DART initial notification worksheet and a BLUE DART authentication call-back script.

D. **Enclosure 2** contains the format to be used by AMC and subordinate commands to frame the body of BLUE DART Threat Warning Acknowledgement Messages and ensure that all MSCs' acknowledgement messages are complete and consistent.

E. **Enclosure 3** contains a Receipt of BLUE DART Threat Warning Checklist to guide the installations' Command Duty Officers in the execution of BLUE DART-associated tasks when addressing a warning on behalf of MSCs.



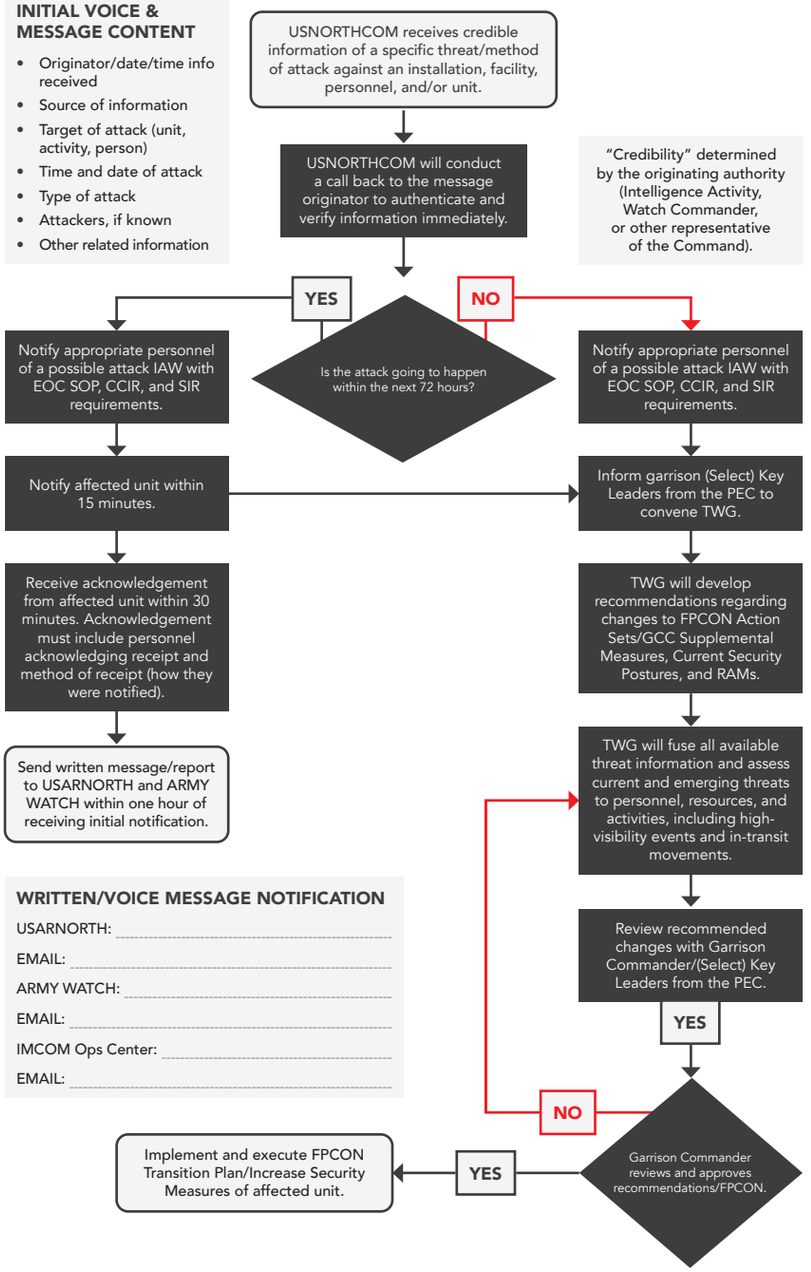
COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BLUE DART/TERRORIST THREAT WARNING

INITIAL VOICE & MESSAGE CONTENT

- Originator/date/time info received
- Source of information
- Target of attack (unit, activity, person)
- Time and date of attack
- Type of attack
- Attackers, if known
- Other related information



WRITTEN/VOICE MESSAGE NOTIFICATION

USARNORTH: _____

EMAIL: _____

ARMY WATCH: _____

EMAIL: _____

IMCOM Ops Center: _____

EMAIL: _____

09-1474-001 USAMC Blue Dart DG.indd 6 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON SYSTEM

The Department of Defense (DoD) FPCON system consists of FPCON levels, which begin with and progress from FPCON ALPHA through FPCON DELTA. Each FPCON level corresponds to an increased probability of a terrorist attack or hostile act, and a corresponding increased specificity of these threats targeting DoD elements and personnel.

When commanders declare an FPCON level, they also employ the appropriate FPCON measures to achieve their desired effects to mitigate the risks from terrorist or hostile act threats.

FPCON ALPHA

OCCURS WHEN THERE IS AN INCREASED GENERAL THREAT OF POSSIBLE TERRORIST ACTIVITY AGAINST PERSONNEL OR FACILITIES, THE NATURE AND EXTENT OF THE THREAT ARE UNPREDICTABLE.

FOR ADDITIONAL INFORMATION CONTACT YOUR SUPERVISOR

FPCON BRAVO

APPLIES WHEN AN INCREASED OR MORE PREDICTABLE THREAT OF TERRORIST ACTIVITY EXISTS.

FOR ADDITIONAL INFORMATION CONTACT YOUR SUPERVISOR

FPCON CHARLIE

APPLIES WHEN AN INCIDENT OCCURS OR INTELLIGENCE IS RECEIVED INDICATING SOME FORM OF TERRORIST ACTION OR TARGETING AGAINST PERSONNEL OR FACILITIES IS LIKELY.

FOR ADDITIONAL INFORMATION CONTACT YOUR SUPERVISOR

FPCON DELTA

APPLIES IN THE IMMEDIATE AREA WHERE A TERRORIST ATTACK HAS OCCURRED OR WHEN INTELLIGENCE HAS BEEN RECEIVED THAT TERRORIST ACTION AGAINST A SPECIFIC LOCATION OR PERSON IS IMMINENT.

100% ID CARD CHECK IS IMMINENT.

FOR ADDITIONAL INFORMATION CONTACT YOUR SUPERVISOR

Source: www.dvidshub.net/image/6012932/understanding-fpcon-status

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON MEASURES

The DoD FPCON system includes FPCON ALPHA through DELTA mandatory measures and GCC-directed FPCON ALPHA through DELTA supplemental measures.

Commanders will:

- Fully implement mandatory measures when FPCON ALPHA through DELTA, respectively, are declared.
- Remind their personnel to be alert for and to report suspicious activities in accordance with DoDI 2000.26, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.
- Educate their personnel on the insider threat to DoD elements and personnel in accordance with the November 21, 2012, Presidential Memorandum and DoDD 5205.16.
- Comply with and integrate DoD physical security and installation access control policies into their FPCON plans.



COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

GENERAL FPCON LEVEL PROCEDURES

Information linking a site and site-specific mitigation measures to an FPCON level is considered controlled unclassified information (CUI) at a minimum. Commanders will ensure that CUI is marked, safeguarded, and disseminated in accordance with Volume 1 of DoDM 5200.01. If the information linking a site and site-specific mitigation measures to an FPCON level is classified pursuant to a security classification guide, then the safeguarding and marking requirements are delineated in DoDM 5205.02-M.

Commanders of installations, separate facilities, and DoD-owned, leased, or managed space in off-installation facilities, including DoD-owned, leased, or managed defense critical infrastructure at those installations and facilities, will supplement each FPCON measure with site-specific details describing how the measure is to be implemented locally, including responsibilities assigned to subordinate units and organizations.

As the threat situation dictates, and as more and more FPCON measures are implemented, commanders will implement additional operations and information security measures to ensure the protection of sensitive and classified information related to implementing their FPCON system.



COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON ALPHA

FPCON ALPHA applies when a general threat of attack, hostile acts, or coercive activities, including gray-zone methods, exists against DoD-affiliated personnel globally, but no specific information indicates a direct or indirect threat to DoD-affiliated personnel.

During FPCON ALPHA, commanders and civilian equivalents:

1. Implement mandatory and supplemental FPCON measures to deter and detect aggression and general, non-specific threats of attacks, hostile acts, and other threats.
2. Prepare to immediately implement additional resilience and security measures designed to detect, delay, deny, and defend against these threats if the likelihood or expected consequences of these threats increase.
3. Must sustain FPCON ALPHA measures indefinitely.

QuickNote

The FPCON System provides DoD Component heads, commands, agencies, and activities the flexibility to adapt FPCON measures based on local threats and coercive activity.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Mandatory Measures

ALPHA 1	Maintain a deliberate and visible RAM program based on local suspicious activity reporting and threat assessments to enhance deterrence and detection efforts.
ALPHA 2	Randomly inspect commercial deliveries to detect and deter hostile actors.
ALPHA 3	Implement notification and communications procedures. Test mass warning, emergency notification, and communications procedures and equipment.
ALPHA 4	Consistent with mission requirements, deter and enhance detection of hostile activity by reducing ground, water, and air access points.
ALPHA 5	Encourage detection and reporting by regularly informing all personnel of the general threat situation, the reason for changes in FPCON measures, and suspicious activity reporting protocols.
ALPHA 6	Identify DoD defense critical infrastructure (DCI) in protection plans and program strategies to deter, detect, deny, delay, and defend these assets.
ALPHA 7	Establish and implement procedures to report indications of hostile actor surveillance of DoD-affiliated personnel.
ALPHA 8	Engage with public and private sector stakeholders to identify infrastructure dependencies. Establish and maintain collaborative relationships to mitigate the effects of interruption or loss of civilian DCI.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON BRAVO

FPCON BRAVO applies when hostile acts, including coercive activities, are escalating or an attack targeting DoD-affiliated personnel is likely, but the specific timing, nature, and targets of these threats cannot be identified.

During FPCON BRAVO, commanders and civilian equivalents:

1. Implement mandatory and supplemental FPCON measures to enhance the deterrence and detection of attacks, hostile acts, and security threats.

2. Prepare to immediately implement supplemental FPCON measures to ensure operational resilience and to deter, detect, delay, deny, or defend against these threats.

3. Must sustain FPCON ALPHA through BRAVO measures indefinitely.



COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Mandatory Measures

BRAVO 1	Deter and detect threats by increasing the frequency of inspections for privately-owned vehicles and their occupants' hand-carried items attempting entry onto DoD installations or facilities owned or controlled by the DoD.
BRAVO 2	Increase the number, concentration, and duration of RAMs based on suspicious activity reporting and threat assessments to enhance deter, detect, deny, and delay efforts.
BRAVO 3	Enhance protection measures for off-installation facilities that support DoD personnel or operations (e.g., recruiting centers, DoD transportation) to detect, deter, and delay hostile adversary planning and movement.
BRAVO 4	Increase the frequency of intelligence and threat information-sharing with DoD intelligence organizations and Federal, State, local, tribal, and territorial agencies.
BRAVO 5	Collaborate with community stakeholders to deter, detect, and delay incidents impacting DoD critical assets and infrastructure interdependencies. Account for authorities, policies, and directives applicable to each agency.
BRAVO 6	Deter hostile actors by increasing the visibility of techniques, tactics, and procedures to present an enhanced protection posture.
BRAVO 7	Consider terminating use of friendly unmanned systems employed for purposes other than FP and law enforcement activities, including terminating unmanned aircraft system (UAS) flights over DoD installations and facilities.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON CHARLIE

FPCON CHARLIE applies when an overt attack or hostile act occurs within the area of interest, or intelligence is received indicating a specific and credible hostile act or targeting against DoD-affiliated personnel or DoD facilities is likely.

During FPCON CHARLIE, commanders and civilian equivalents:

1. Implement mandatory and supplemental FPCON measures designed to delay and deny attacks and overt hostile acts.
2. Implement additional plans and procedures to detect, defend against, respond to, and recover from these increased threats.
3. Must sustain FPCON ALPHA through CHARLIE measures until the threat is mitigated.

QuickNote

FPCON mandatory measures are cumulative (e.g., declaration of FPCON CHARLIE includes implementation of all FPCON ALPHA, BRAVO, and CHARLIE mandatory measures, unless otherwise directed by the FPCON declaring authority).

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Mandatory Measures

CHARLIE 1	Increase standoff distance where possible to defend critical facilities, soft targets, and mass gathering facilities that are vulnerable to identified threats and anticipated tactics.
CHARLIE 2	Deter unauthorized access and detect hostile attempts by conducting inspections of all commercial vehicles, including their drivers and occupants, entering DoD installations or facilities owned or controlled by the DoD.
CHARLIE 3	Increase explosive and chemical, biological, radiological, and nuclear detection capabilities at access control points, as resources permit.
CHARLIE 4	Deter, detect, and delay hostile activity by unmanned systems through supplementary lighting, barriers, and obstacles.
CHARLIE 5	Deter unauthorized access by limiting the number of installation and DoD facility perimeter access points, including access to DoD DCI, and increase detection capabilities at likely avenues of approach.
CHARLIE 6	Suspend the trusted traveler program in accordance with Volume 3 of DoD Manual 5200.08.
CHARLIE 7	Terminate use of friendly unmanned systems employed for purposes other than FP and law enforcement activities, including UAS flights over DoD installations and facilities.
CHARLIE 8	Implement mitigation plans and measures to rapidly reconstitute critical mission capabilities.
CHARLIE 9	Distribute operations through use of alternate sites and telework.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FPCON DELTA

FPCON DELTA applies when an attack or overt hostile act has occurred or is imminent against specific installations or operating areas.

During FPCON DELTA, commanders and civilian equivalents:

1. Implement mandatory and supplemental FPCON measures to respond to, defend against, and recover from the attack or hostile act, and prevent follow-on attacks.
2. Stop all non-essential support functions, operations, and movement.
3. Implement FPCON measures in accordance with DoDD 5210.56 and CJCS Instruction 3121.01.
4. Must sustain FPCON ALPHA through DELTA measures until the threat is mitigated. Maintain FPCON DELTA only as long as the response capabilities are required to respond to or eliminate the threat.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Mandatory Measures

DELTA 1	Delay and deny hostile activity by limiting access to installations, DoD facilities, and DoD DCI to mission-essential personnel determined by the commander.
DELTA 2	Maximize detection and deterrence by inspecting all vehicles and personnel entering installations or facilities not identified by the commander as operationally exempted (e.g., credentialed members of the Military Criminal Investigative Organizations or members of the Military Department Counterintelligence Organizations).
DELTA 3	Restrict all non-essential movement on DoD property.
DELTA 4	Implement detection procedures to positively identify all personnel circulating on installations and in facilities without exception.
DELTA 5	Fully activate contingency plans and direct available resources to defend against an attack.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BOMB THREAT

This checklist is designed to help employees and decision-makers of commercial facilities, schools, etc., respond to a bomb threat in an orderly and controlled manner with first responders and other stakeholders.

Most bomb threats are received by phone. Act quickly but remain calm and obtain information with the checklist on the following pages.

QuickAlert

Bomb threats are serious until proven otherwise.

If a bomb threat is received by phone:

- Remain calm. Keep the caller on the line for as long as possible. **Do not hang up**, even if the caller does.
- Listen carefully. Be polite and show interest.
- If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
- If your phone has a display, copy the number and/or letters on the window display.
- Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
- Immediately upon termination of the call, **do not hang up**, but from a different phone, contact authorities immediately with information and await instructions.

QuickContact

For more information, contact the Office for Bombing Prevention at **OBP@cisa.dhs.gov** or visit: **https://cdp.dhs.gov/obp**

09-1474-001 USAMC Blue Dart DG.indd 18 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

If a bomb threat is received by handwritten note:

- Call:
- Handle the note as minimally as possible.

If a bomb threat is received by email:

- Call:
- Do not delete the message.

Signs of a Suspicious Package

- No return address; poorly handwritten address; misspelled words
- Incorrect titles
- Excessive/foreign postage
- Stains; strange odor
- Unexpected delivery
- Restrictive notes

Refer to your local bomb threat emergency response plan for evacuation criteria.

QuickAlert ⚠

Radio signals have the potential to detonate a bomb. Avoid using two-way radios or cellular phones. Also, avoid touching or moving a suspicious package.

09-1474-001 USAMC Blue Dart DG.indd 19 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BOMB THREAT CHECKLIST

Date:	Time Caller Hung Up:
_____ /___ /___	_____
Time:	Phone Number Where Call Was Received:
_____	_____

If a bomb threat is received by email:

- Where is the bomb located (building, floor, room, etc.)?

  _____

- When will it go off?

  _____

- What does it look like?

  _____

- What kind of bomb is it?

  _____

- What will make it explode?

  _____

- Why?

  _____

- What is your name?

  _____

Exact Wording of Threat:

_____

_____

09-1474-001 USAMC Blue Dart DG.indd 20 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED = PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Information About Caller:

- Where is the caller located (background/level of noise)?

- Estimated age:

- Is the voice familiar? If so, who does it sound like?

- Other points:

Caller's Voice	Background Sounds	Threat Language
☐ Female	☐ Animal noises	☐ Incoherent
☐ Male	☐ Booth	☐ Irrational
☐ Accent	☐ Clear	☐ Message read
☐ Calm	☐ Conversation	☐ Profane
☐ Clearing throat	☐ Factory machinery	☐ Taped message
☐ Coughing	☐ House noises	☐ Well-spoken
☐ Cracking voice	☐ Kitchen noises	
☐ Crying	☐ Local	
☐ Deep	☐ Long distance	
☐ Deep breathing	☐ Motor	
☐ Disguised	☐ Music	
☐ Distinct	☐ Office machinery	
☐ Excited	☐ PA system	
☐ Laughter	☐ Static	
☐ Lisp	☐ Street noises	
☐ Loud		
☐ Nasal	**Other Information:**	
☐ Normal		
☐ Ragged	---	
☐ Rapid		
☐ Raspy	---	
☐ Slow		
☐ Slurred	---	
☐ Soft		
☐ Stutter		

09-1474-001 USAMC Blue Dart DG.indd 21 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

ENCLOSURES AND FORMATS

Enclosure 1: BLUE DART Initial Notification Worksheet

1. Confirm that this is an ACTUAL or EXERCISE BLUE DART threat warning.

2. This is _____ from USNORTHCOM, ETC., and my telephone number is _____-_____-_____. *Actual commercial line for NORAD-USNORTHCOM is **719-554-9100**.

3. We have information that there may be an attack on (unit, installation, or activity)

   _____.

4. We believe the attack will take place at (date and time)

   _____.

5. The attacker will use (type or means of attack)

   _____.

6. We believe the attack will be conducted by (name of attacker/ organization)

   _____.

7. We believe the attack will be conducted because

   _____.

8. The source of this information is

   _____.

9. Record the time that the initial notification was completed (time) _____. YOU MUST NOW AUTHENTICATE THE INITIAL NOTIFICATION USING THE AUTHENTICATION CALL-BACK SCRIPT ON THE NEXT PAGE.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BLUE DART Authentication Call-Back Script

1. Call the person you identified in line 2 of the BLUE DART Initial Notification Worksheet on the previous page.
2. Identify your call as an ACTUAL or EXERCISE BLUE DART threat warning authentication.

   ---

3. This is _____ from (Command Installation Watch Officer), calling to authenticate a BLUE DART threat notification that I have received from (name of person who rendered initial notification)

   ---

4. I understand that there may be an attack on (unit, installation, or activity)

   ---

5. I understand that the attack will take place at (date and time)

   ---

6. I understand that the attacker will use (type or means of attack)

   ---

7. I understand that the attack will be conducted by (name of attacker/organization)

   ---

8. I understand that the attack will be conducted because

   ---

9. I understand that the source of this information is

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Enclosure 2: Format of MSC Commander's Receipt of BLUE DART Acknowledgement Message

UNCLASSIFIED/CUI//

MSGID/GENADMIN/***CO INSTALLATION PLAD/MSG REF NO#/ MONTH YEAR//***

SUBJ/OPREP-3/BLUE DART/MCIEAST/ACKNOWLEDGEMENT//

REF/A/USNORTHCOM Instruction 10-211/15MAR19//

POC/CDO INSTALLATION/TEL: ***CML/***TEL: ***DSN/***EMAIL:

EXERCISE/EXERCISE/EXERCISE// ***(Use only during an exercise.)***

GENTEXT/REMARKS/1. AT _____ ***DTG*** _____ THE INSTALLATION CDO ***(PRI POC)*** RECEIVED A BLUE DART NOTIFICATION CONTAINING THE FOLLOWING INFORMATION:

1.A. THE NOTIFICATION WAS MADE BY ***(initial POC & contact data)*** FROM USNORTHCOM ***(or identify the actual Command title).***

1.B. THE MEANS OF NOTIFICATION WAS BY TELEPHONE/ SECURE TELEPHONE/AMHS MESSAGE ***(identify the actual media used).***

2. THE BLUE DART THREAT NOTIFICATION INCLUDED THE FOLLOWING INFORMATION:

2.A. AN ATTACK ON ***(name/location of target installation).***

2.B. THE ATTACK WILL TAKE PLACE AT ***(time/date).***

2.C. THE ATTACKER(S) WILL USE ***(method of attack).***

2.D. THE ***(name of attacker if known).***

2.E. THE ATTACK IS BEING CONDUCTED BECAUSE ***(if known).***

2.F. THE SOURCE OF THE THREAT INFORMATION IS ***(if known).***

3. ***CO INSTALLATION PLAD*** HAS INITIATED THE LOCAL NOTIFICATION OF STAFF AND TENANT COMMANDS. //

EXERCISE/EXERCISE/EXERCISE ***(Use only during an exercise.)***

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Enclosure 3: Receipt of BLUE DART Threat Warning Checklist

Sequence	Task	Notified Y/N	Person Contacted	Time
1.	Receive initial BLUE DART warning. Ensure that you fill out all blocks of the Initial Notification Worksheet.			
You have 15 minutes to complete steps 2-4.				
2.	Execute Authentication Call-Back to USNORTHCOM using the Authentication Call-Back Script.			
3.	**If BLUE DART is received after normal working hours, week-ends, and holidays, voice notification will be made to the CMD Operations Center (COC).			
4.	**If BLUE DART is received during normal working hours, notify the OPS Center, AMC OPS Center.			
You have 60 minutes to complete steps 5.1.-5.5.				
5.1	Prepare Acknowledgement Message in Naval Message format in a Word document and send as an attachment *.docx or *.pdf to the following:			

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BLUE DART Telephonic Reporting Format

1. Mandatory Lines

   - "This is a real-world BLUE DART terrorist threat warning."
   - "This is (caller's identity) from (organization) and my unit telephone number."
   - "We have information there may be a terrorist attack on (location/person)."
   - "We believe the attack will take place at (time/date)."
   - "The attacker will use (type of weapon) and the (method of attack)."

2. Additional Information to Provide (if known)

   - "(Identity of attacker) will conduct the attack."
   - "The attack is being conducted because (reason for attack)."

3. Optional Information to Provide

   - Source of the information (general description of source's position, access, and reliability).

QuickNote

Only identify source if secure communications are available and classification/dissemination restrictions are satisfied.

09-1474-001 USAMC Blue Dart DG.indd 26 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BLUE DART Follow-up Message Format

(Appropriate Classification of Message)

FROM: (Sending unit) TO: (Targeted unit)

INFO: (Up, down, cross-echelon commands as appropriate)

SUBJECT: (U) BLUE DART Follow-up Report

1. (U) **THREAT.** Specific information concerning terrorist attack, which will include the following: (*Ensure document and paragraphs are properly marked.)
   - (U) Specific unit, individual, or location to be attacked (mandatory)
   - (U) Specific time and date of attack (mandatory)
   - (U) Specific threat or method of attack to be used (mandatory)
   - (U) Identity of attacker(s) (if known)
   - (U) Reason for the attack (if known)
2. (U) **SOURCE.** Original information source. Provide source description, access, and assessment of source's reliability. (Do not include source if it is not necessary in order to prevent compromise.)
3. (U) **CHRONOLOGY.** Events since reception of information to include notification of affected target.
4. (U) **ORIGINATOR.** Identity of individual who initially acquired the information, time information was obtained, and telephone contact number(s) to the message sender's command center or watch.

09-1474-001 USAMC Blue Dart DG.indd 27 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

U.S. Army Materiel Command (AMC) BLUE DART PROGRAM

for Major Subordinate Commands

BLUE DART is an antiterrorism (AT) threat warning program designed to rapidly disseminate threat information directly to affected areas and units. This handbook establishes procedures to guide AMC installations, units, or activities in the execution of duties connected with the BLUE DART notification system.

- BLUE DART message procedures
- FPCON mandatory measures
- Bomb threat checklist
- Reporting and call-back message formats

Point of Contact:
Martin Oglesby
HQAMC, G-3 Protection Branch
Redstone Arsenal, AL
martin.oglesby.civ@army.mil

Photos used for illustrative purposes only; the people shown are not linked to the topic.

© 2026 QuickSeries Publishing
1-800-361-4653 | www.quickseries.com

01-1474-100-01 | 1474-001
ISBN 978-1-62350-051-1 | Printed in Canada

09-1474-001 USAMC Blue Dart DG.indd 28 2026-02-02 1:32 PM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.