DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5510.1A
N1
15 JUN 12

CNATRA INSTRUCTION 5510.1A

Subj: COMMAND SECURITY POLICY MANUAL

Ref: (a) SECNAV M-55l0.30
(b) SECNAV M-5510.36
(c) SECNAV M—5210.1

Encl: (1) General Information
(2) Personnel Security
(3) Information Security
(4) Emergency Action Plan
(5) Bomb Threat Checklist

1. Purpose. To standardize procedures employed in the handling of classified material for Chief of Naval Air Training (CNATRA) staff, with the goal of preventing the compromise of classified material per references (a) through (c). This instruction is published per references (a) and (b) to ensure complete control and accountability of the command security program and all classified material.

2. Cancellation. CNATRAINST 5510.1.

3. Scope. This instruction applies to all personnel attached to CNATRA and forms the basis for the staff's control and dissemination of classified material. This instruction is a supplement to references (a) and (b) and sets a more restrictive command policy. Enclosures (1) through (5) are provided to assist staff personnel with the execution of this instruction.

C. HOLLINGSWORTH
Chief of Staff

Distribution:
CNATRA Website

GENERAL INFORMATION

1. Responsibility. The Chief of Staff (COS) is responsible for compliance with and implementation of the Department of the Navy (DON) Personnel Security Program (PSP) and Information Security Program (ISP). Individuals appointed to the following positions shall be designated in writing by the COS:

a. The Command Security Manager (CSM) is key in developing and administering the command's ISP and PSP. The CSM is the principal advisor on information and personnel security in the command except for issues specific to Special Compartmentalized Information (SCI) and Special Access Programs (SAPs) unless officially designated for these additional duties and responsibilities.

b. The Assistant Command Security Manager (ACSM) will provide assistance to the CSM in the execution of his stated duties.

c. The Classified Material Control Officer (CMCO) is responsible to the CSM for the receipt, reproduction, transfer, transmission, and destruction of command SECRET and CONFIDENTIAL material.

d. The Top Secret Control Officer (TSCO) is responsible to the CSM for the receipt, reproduction, transfer, transmission, and destruction of command TOP SECRET material.

e. The Information Assurance Manager (IAM) is responsible to the CSM for protection of classified information being processed in Automated Data Processing (ADP) systems, and responsible to the Physical Security Officer for the protection of ADP equipment and related resources.

f. Assistant Chiefs of Staff (ACOS) are responsible to the CSM for ensuring that all classified material in their department is properly controlled and safeguarded.

g. Safe Custodians will be designated by ACOS's to the CMC. Safe Custodians are responsible to their ACOS's for ensuring all classified material containers in their spaces are properly and securely maintained as outlined in paragraph 8 of enclosure (3). A maximum of four Safe Custodians may be designated per safe.

2. Accountability. Security of classified material is a basic responsibility of all CNATRA personnel. Individuals who have custody of classified material are responsible for the safeguarding of that material and are subject to disciplinary action if that material is lost or otherwise compromised.

PERSONNEL SECURITY

1. Check-in/Check-out Procedures. All Personnel assigned to CNATRA shall check in and out with the CSM or ACSM.

a. Check-in. Personnel will be notified at this time if their eligibility for access has expired. If eligibility for access has expired, a request for a re-investigation will be initiated and the member will be given directions on how to access and complete their Electronic Questionnaires for Investigations Processing (EQIP).

(1) Military personnel. During the check-in process the CSM or ACSM will gain the member in JPAS and determine, the level of access that will be granted based on the individual's billet, eligibility, and need to know. The member will receive a verbal security briefing and sign a Non-disclosure Agreement (SF-312), if one is not already documented in JPAS.

(2) Civilian personnel. During the check-in process the CSM or ACSM will gain the employee in JPAS and determine the level of access that will be granted based on the individual' s Position Description (PD), eligibility, and need to know. The employee will receive a verbal security briefing and sign a SF-312, if one is not already documented in JPAS.

(3) Contractor personnel. During the check-in process the CSM or ACSM will gain the employee in the JPAS and determine the eligibility level the individual holds. Upon determining the member's eligibility level, the CSM or ACSM will inform the Contractor Verification System (CVS) Trusted Agent (TA) of their eligibility.

b. Check—out. During the check-out process all personnel will be released in JPAS and their command security files will be destroyed. All military personnel who are separating and all civilian personnel who have terminated their employment must sign an OPNAV Form 5511/14.

2. Personnel Security Investigations (PSI). The CSM and ACSM will continually review CNATRA personnel eligibility, and need to know. Notification will be made to individuals as they are required to submit re-investigation packages.

3. Building Access. Requests for access to CNATRA headquarters building will be submitted to the CSM or ACSM. Requests must be submitted by active duty military or DOD employees. Contractors are not permitted to request building access for personnel.

4. Visit Requests. Per current DOD and DON policies all outgoing and incoming visit requests must be sent via JPAS. Personnel in need of a visit request must submit a formal request to the CSM or ACSM for transmittal.

5. Training and Education. The CSM is responsible for implementing an ongoing program to ensure all personnel receive education and training in the proper handling of classified material. The program will consist of:

a. Indoctrination briefing during command check-in.

b. Annual refresher briefings.

c. Standardization meetings with ACOS’s when procedural changes occur or when the CSM becomes aware of unsafe practices.

d. Records of training shall be maintained by the CSM.

INFORMATION SECURITY

1. Management. Accounting for classified material will be as follows:

a. TOP SECRET. The TSCO shall maintain control records individually tracking all TOP SECRET material from receipt to destruction or transfer. Full accounting procedures for TOP SECRET material are outlined in paragraph 3a.

b. SECRET. The CMCO shall maintain control records individually tracking all SECRET material from receipt to destruction or transfer. Full accounting procedures for SECRET material are outlined in paragraph 3b.

c. CONFIDENTIAL. There are no requirements for control records on CONFIDENTIAL material. However, the unauthorized disclosure of this material could cause damage to nationa1 security and under no circumstances should safeguarding of this material be overlooked.

d. NO FOREIGN NATIONAL (NOFORN). A special handling instruction, NOFORN material should be provided sufficient safeguarding to offer complete control of personnel accessing the material and prevention of release to a foreign national.

e. FOR OFFICIAL USE ONLY (FOUO). Although not considered “classified” FOUO is considered privileged and should not be disclosed without proper need to know. All personnel are charged with limiting dissemination of this material.

2. Distribution. Departments will be notified by the CMCO when classified material is received and addressed to their department. Notification will be affixed to the department’s mail box in Admin. If a department does not respond to the notification within 14 working days or if the department determines the material is not needed, it will be destroyed by the CMCO.

3. Receipt and Records Control. Classified material shall be controlled based on the classification of the material. TOP SECRET and SECRET material shall be individually controlled and tracked by the CMCO and TSCO. All classified material received by the command must be processed through the CMCO/TSCO.

a. TOP SECRET. Upon receipt of TOP SECRET material, the TSCO shall:

(1) Page check the document and sign the Record of Page Checks inside the document. A Record of Page Checks shall be added if not included in the document.

(2) Log the material into the TOP SECRET inventory by assigning the next available control number and entering the date of receipt, title, originator, copy number, and subject into the log.

(3) Print a custody sheet. The custody sheet must be signed by the individual that will be responsible for safeguarding the material. Typically, this will be the TSCO or their assistant. The custody sheet must be kept with the material at all times.

(4) Control stamp, in red ink, the document's front cover and the first page after the cover. The stamp will then be filled in with the TOP SECRET control number and copy number.

(5) If the document is not clearly marked attach an SF-703 (Top Secret Cover Sheet) to the front and back of the document. TOP SECRET stickers shall be attached to the spine, if possible, to ensure the classification can be seen regardless of the orientation of the document.

(6) Scan for any action required and advise the chain of command as required. There will be no standard routing for TOP SECRET material.

(7) Place the material in the TOP SECRET safe.

b. SECRET. Upon receipt of SECRET material, the CMCO shall:

(1) Page check each item to ensure completeness.

(2) Log the material into the SECRET inventory by assigning the next available control number and entering the date of receipt, title, originator, copy number, and subject into the log.

(3) Print a custody sheet. The custody sheet must be signed by the individual that will be responsible for safeguarding the material, typically, the CMCO or their assistant. However, if the material is required by another code, an Internal Transfer Sheet shall be prepared and signed by the code's Security Clerk upon their receipt of the material.

(4) Control stamp, in red ink, the document's front cover and the first page after the cover. The stamp will then be filled in with the SECRET control number and copy number.

(5) If the document is not clearly marked, attach an SF-704 (Secret Cover Sheet) to the front and the back of the document. SECRET stickers shall be attached to the spine if possible, to ensure classification can be seen regardless of the orientation of the document.

(6) File the registered mail receipt in the incoming binder and mail the return receipt.

(7) Scan the document for any action required and notify the appropriate department that the material has arrived. There will be no standard routing for SECRET material.

(8) Place material in the vault.

(9) File the Internal Transfer Sheet in the code's file.

4. Marking. All classified information shall be clearly marked with the appropriate classification level and all required "associated markings." Chapter 6 of reference (b) sets forth the marking requirements for all classified material. All classified material produced within CNATRA will be marked as "Derived from" as CNATRA does not have Original Classification Authority (OCA). The phrase "Multiple Sources" may be used when classification is derived from more than one source. A listing of the sources must be maintained with the file copy of the document.

5. Dissemination. Dissemination of all classified material shall be kept to the absolute minimum necessary for proper conduct of operations. Access to classified information is based upon proper clearance and "need-to-know." Individuals must possess a clearance commensurate with the information they require access to and must be granted access by the command.

6. Command Inventory. An inventory is a means to account for all material assigned to an individual, container, or the command. Reference (b) requires an annual inventory of all classified material. The Admiral, COS, and CSM may order an inventory at any time. The procedures for a command inventory are as follows:

a. The inventory will be frozen and no classified material will be transferred until the inventory is complete.

b. Two properly cleared personnel shall conduct the inventory. CMCO/TSCO will attempt to provide a representative to conduct the inventory.

c. Each item on the inventory shall be sighted by both personnel and marked as accounted for, including items on sub-custody. TOP SECRET material must be page checked to ensure completeness. If a discrepancy is discovered, report it to the CMCO/TSCO immediately.

d. Once all items are inventoried, both personnel shall sign and date the inventory sheet.

NOTE: PERSONNEL CONDUCTING THE INVENTORY MUST BE AWARE THAT THEIR SIGNATURE INDICATES THAT ALL ITEMS WERE SIGHTED, AND THEY MUST UNDERSTAND THAT DISIPLINARY ACTION MAY BE TAKEN AGAINST THEM IF AN INVENTORY IS FALSIFIED.

e. When the inventory is complete, the CMCO/TSCO will submit a report to the COS. The report will include the results of the inventory and what actions have been taken regarding any unresolved discrepancies.

7. Safeguarding. Classified material must be safeguarded in a manner to deny access to unauthorized personnel.

a. Classified material shall be locked in a GSA approved storage container or under the direct supervision of authorized personnel at all times. DO NOT leave classified material unattended under ANY circumstances.

b. Classified material shall not be viewed, discussed, or displayed in public areas such as the passageway, ladder well, etc.

c. When transporting classified material within the command, personnel will take reasonable precautions to prevent inadvertent disclosure including using a cover sheet, file folder, or other covering. UNDER NO CIRCUMSTANCE is classified material to be carried in such a way as to permit casual observance.

d. Classified material shall not be removed from command spaces unless specifically approved by the CSM. A Command Authorization Letter and/or Courier Card are required after CSM approval. Transportation of classified material is outlined in paragraph 11.

e. At the end of the day, the CSM or ACSM shall ensure that all classified materials, including working papers, computer disk/CDs, hard drives, printer/typewriter ribbons, and burn bags, are properly stored and all safes are locked. XO locks shall be spun until a lightning bolt indication appears and then an attempt will be made to open each drawer of the container. An SF-702 (Activity Security Checklist) will be signed after these tasks are completed.

f. End of Day checks also include ensuring computer equipment is turned off, waste baskets contain no classified material and all windows and doors are securely locked. When all of the above tasks are completed and the space is to be secured for the day, an SF-701 (Security Container Information Form) will be completed by the last person leaving the space.

8. Storage. Only containers inspected and approved by the CSM for storage of classified material will be utilized.

a. Safes. Command safes are cleared for storage of classified material up to and including SECRET. TOP SECRET must be stored by the CMCO/TSCO. An SF-700 shall be completed. Attach the top copy inside the safe per reference (b). The combination card will be legibly completed and sealed in the envelope portion of the SF-700. The envelope will be stamped with the highest classification of the material protected within the safe and returned to the CMCO for storage.

b. Combinations. Safe and lock combinations shall be handled per reference (b). An SF-700 containing the combinations of all safes safeguarding classified material shall be maintained in the CSM's vault. The SF-700 containing the CSM's vault combination shall be maintained in the Admin Officers safe. Each time a person with knowledge of a safe combination no longer requires access to that safe; the safe combination shall be changed unless access can be denied by other means (i.e., cipher lock). At a minimum, safe combinations shall, be changed annually.

9. Reproduction. Classified material shall only be reproduced on equipment that is approved by the CSM for the appropriate level of material being copied. All SECRET material that is reproduced must be processed through CMCO/TSCO and added to the inventory per receipt procedures outlined in paragraph 3.

a. CONFIDENTIAL: Reproduction of CONFIDENTIAL material must be approved by the Department Head, CSM, or CMCO.

b. SECRET: Reproduction of SECRET material requires the authorization of the Admiral, COS, CSM or CMCO.

c. TOP SECRET: Reproduction of TOP SECRET material is strictly prohibited unless authorized in writing by the OCA. The TSCO shall be involved in all TOP SECRET reproduction.

d. All copiers authorized for reproduction of classified material will conspicuously display the maximum level of classification the copier may be used to reproduce. Warning notices will be affixed per reference (b).

10. Transfer. To transfer material out of the command, CMCO/TSCO must be involved. Individuals are not authorized to transfer material without CMCO/TSCO involvement. To permanently transfer SECRET material within the command, the individual transferring the SECRET material must turn it in to the CMCO/TSCO for transfer to the receiving individual.

11. Transportation. When an individual requires use of classified material outside command spaces, CSM, COS, or Admiral approval is necessary to authorize transport and CMCO/TSCO must prepare a Command Authorization Letter and/or Courier Card.

a. Transportation of classified material will only be approved when the classified material is required at the traveler's destination, is not available at the location to be visited, and cannot be transmitted by other authorized means due to time or other constraints.

b. If approved, the transportation of classified material must comply with reference (b), Hand Carrying Procedures, and will be performed per the following:

(1) The courier must report to CMCO/TSCO to receive a transportation brief and Command Authorization Letter/Courier Card.

(2) The classified material shall be wrapped, all seams sealed, addressed, and marked with the highest classification contained in the package. The material shall then be wrapped in an outer wrapper, all seams sealed and outer wrap addressed. In order to ensure compliance with the wrapping requirements of reference (b), all wrapping should be performed by CMCO/TSCO.

(3) The classified material must be in the courier's physical possession at all times, unless properly stored at a U.S. Government activity in a GSA approved container.

(4) Do not read, study, display, or use classified material in any manner on a public conveyance or in a public place.

(5) When the classified material is carried in a private, public, or government conveyance, do not store it in any detachable storage compartment, such as an automobile

luggage rack. When traveling on a commercial aircraft DO NOT store the classified material in the overhead storage compartments. Material shall not be left unattended in a vehicle at any time including the locked trunk of a car.

(6) A list of all classified material carried by the member will be maintained by CMCO/TSCO. Upon the members return that individual shall be required to account for all of the classified material.

12. Transmission. When classified material needs to be transferred between commands either electronically (i.e., computer to computer) or via fax machine, the transfer must be accomplished via secure lines.

13. Mailing. At times, classified material will need to be transferred via mail or courier. All classified mail will be brought to CMCO. CMCO will ensure the package containing classified material is packaged per reference (b) prior to its mailing.

14. Destruction. Per reference (b), classified documents and material that are not permanent valuable records of the government shall not be retained for more than five years from the date of origin, unless such retention is authorized per reference (d). During command inventories and clean—out days, a portion of the work performed in each office will be devoted to the disposal of unneeded classified holdings.

a. CMCO/TSCO shall serve as central repository for all TOP SECRET and SECRET material destined for destruction. All TOP SECRET and SECRET destruction in the command will be performed by CMCO/TSCO personnel.

b. Destruction of classified material requires two appropriately cleared individuals during the entire destruction process, including the transportation of burn bags.

c. A Record of Destruction Certificate, listed by control number, shall be printed before the destruction of TOP SECRET or SECRET material commences.

d. TOP SECRET material must be page checked prior to destruction.

e. Destruction methods are:

(1) Cross-cut Shredder. The primary means of destruction shall be a GSA approved cross-cut shredder. Cross-cut shredders must be inspected and authorized by the CSM.

(2) Burn Bags. Burn bags are only authorized in extreme circumstances (i.e., broken shredder or none available). Burn bags will be used per the following procedures:

(a) Burn bags will be safeguarded at the level of the highest classification they contain.

(b) When a burn bag is no longer needed or becomes full, it will be sealed, serialized per the next number in the "Burn Bag Log," and signed by two appropriately cleared witnesses. A record of all subsequent handling and storage will be maintained to prevent unauthorized disclosure prior to destruction.

(c) The destruction of burn bags will be recorded by the serial number (determined by the Burn Bag Log) on an OPNAV 5511/12, Classified Material Destruction Report. The 5511/12 will be signed by the two appropriately cleared witnesses performing the destruction and will be attached to the record of handling.

(d) The record of handling and Classified Material Destruction Report will be maintained for two years after the destruction.

f. Emergency Destruction. A copy of enclosure (4) shall be posted in each office where classified material is stored. This plan provides for the destruction of classified material in the event of a natural disaster or civil disturbance.

15. Security Violations. Security violations include loss or compromise of classified information. Compromise is the exposure of classified material to unauthorized personnel. A security incident is any act or procedure that results in, or may result in, an actual or possible compromise of classified material. If classified material is not under complete control, there exists the possibility that unauthorized disclosure has occurred.

a. Any possible security incident shall be reported to the CMCO/TSCO, the CSM, and the COS. The COS shall be notified of all security incidents, even if a determination of "no compromise" is made.

b. If classified material is discovered unattended, take control of the material and contact the CMCO/TSCO or CSM. If classified material is discovered unattended or a security container is found unsecured during non-working hours, carry out the following procedures:

(1) The person making the discovery shall immediately notify the SDO. The SDO shall immediately notify the CMCO/TSCO, and the CSM.

(2) A guard must be continuously posted from the time of discovery until the CMCO or CSM arrives and assumes custody of the material or the container. The CMCO or CSM will inventory the container and contact the Chief of Staff.

(3) The SDO shall ensure appropriate log entries are made to document the event.

c. When a security violation, is discovered, an investigation shall be conducted to determine the probability of compromise. All investigations will follow procedures set forth in Chapter 12 of reference (b).

16. Working Papers. Working papers are documents and material accumulated or created while preparing finished material (i.e.,' rough drafts). In addition, classified notes from training, meetings and conferences are working papers.

a. When working papers contain classified information, the accounting and marking requirements prescribed for the classification may be modified. As a minimum, working papers shall be:

(1) Marked with the annotation "Working Papers" and the date they are created.

(2) Marked on each page with the highest classification of any information they contain.

(3) Protected per the classification assigned.

(4) Destruction must be ensured once they are no longer needed.

b. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers are:

(1) To be released by the originating department outside the command, transmitted via fax, or transmitted through communication center channels.

(2) To be retained more than 180 days from the date of origin.

(3) To be filed permanently.

c. Working papers meeting any of the criteria in paragraph (b) above will be delivered to the CMCO for proper accounting and control. ACOS’s should advise the CMCO of any working papers delivered for control and accounting that require priority handling. The CMCO will coordinate with the ACOS’s to arrange rapid return of those documents.

EMERGENCY ACTION PLAN

1. The purpose of the Emergency Action Plan is the prevention of unauthorized access/disclosure to classified material issued to or held by CNATRA.

2. The following guidance is provided in the event of emergency, accident or hostile action:

a. Power/Alarm Outage. Should a power failure occur during normal working hours, personnel should ensure all open security containers are properly secured until reactivation of the power supply.

b. Natural Disasters. Should a natural disaster occur during working hours (i.e., tornado, flood, earthquake, etc.), the CSM will assess the situation and determine if evacuation/destruction of classified material and equipment is required.

(1) During non-working hours, the CSM will be notified by the SDO of the situation and will determine if a need exists to evacuate the classified material to a safer location. If evacuation of the classified material is deemed necessary, the CSM will coordinate the attaining of vehicles for the evacuation.

(2) Whenever possible, maintain the classified material within its respective security container during the evacuation in order to help minimize loss or compromise of classified material.

c. Fire Procedures. During a fire, the first rule to observe is to save lives, then protect the classified material. Do not deny fire-fighting personnel admittance to an area because classified material has not been properly secured. However, after notifying the fire department, personnel must make every effort to place classified material in the proper storage containers. After the fire is out, the CSM will be the first to enter the effected spaces to determine possible compromise of classified material not secured and not completely destroyed by the fire. The CSM will also obtain the names of all fire-fighting and emergency personnel who had access to the facility for a debriefing.

(1) If a fire exists within a respective building but not within the immediate area of classified material holdings, office spaces will be sanitized ensuring all classified material has been secured and ADP equipment has been powered down.

(2) Should the fire originate in an area where classified material is held, the first person to detect the fire will alert all personnel and notify the base fire department. If the fire is of such magnitude that fighting the fire with a hand held fire extinguisher is not possible, the area will be evacuated immediately with the door placed in the open position.

(3) After the fire has been contained, personnel will inventory and evacuate all classified material to a secure area. The CSM will notify the chain of command of the extent of the damage, loss of classified material, present location of the material, evaluation of the potential compromise of the material and status of classified holdings. In the event of actual compromise of classified material, notify the local Naval Criminal Investigative Service (NCIS) office at 361-939-2918 or 361-939-2919.

d. Civil Unrest. All personnel are cautioned NOT to discuss classified activities. This caution is an attempt to maintain a low profile in order to not jeopardize or place CNATRA and/or subordinate commands in a position to be singled out by groups or individuals for retaliation of any sort against the U.S. Government. However, should a demonstration within the immediate area occur, all classified material will be secured until further notice by the chain of command.

(1) The SDO, upon notification of a demonstration, will notify the CSM and TSCO. Personnel will not attempt to maintain crowd control, converse with, provoke the demonstrators, or prevent forcible entry. The security police are responsible for maintaining law and order. Personnel will comply with orders and be constantly aware of events surrounding them for debriefing by the appropriate authorities within five working days following the demonstration.

(2) If an evacuation is required to a CNATRA building, upon re-entry of the spaces a complete inventory will be taken and results of inventory will be provided to the CSM.

e. Personal Injury. Should an individual be injured or suffer a disabling injury (i.e., stroke, electrical shock, etc.) in a classified material area, all life saving attempts should be made. However, personnel should make no attempt to move the injured person. Call 911. Proceed to sanitize the area to the maximum extent possible prior to the arrival of emergency/ambulance personnel. Admittance of emergency personnel will not be delayed because of a need for sanitization of the area. In the event that emergency personnel view classified material and/or classified equipment, names of the emergency personnel will be obtained and provided to the CSM for a required debriefing within five days of the incident.

f. Bomb Incidents. Bomb threats are periodically made against military facilities. All personnel should be prepared to react to this situation.

(1) All telephones will have a “Bomb Threat Checklist”, enclosure (5), in the immediate area.

(2) Individual receiving the call will follow the checklist to extract as much detail as possible.

(3) Notify security police.

(4) Implement an immediate evacuation of the area ensuring all classified material has been properly secured prior to departing.

g. Emergency Evacuation Procedures. If the situation dictates the need to remove classified material/equipment from the area, the CSM and TSCO will coordinate the attaining of vehicles for the evacuation and transportation of material.

h. Emergency Destruction Procedures. Should an emergency arise that requires immediate destruction of classified material, the CSM and TSCO will implement emergency destruction procedures.

(1) If an Emergency Destruct is deemed necessary it will be conducted per reference (b).

(2) Material will be destroyed in priority order utilizing approved shredders and burning.

(3) The priority in which classified material will be destroyed is as follows:

(a) Priority One - TOP SECRET

(b) Priority Two – SECRET

(c) Priority Three - CONFIDENTIAL

(4) After destruction, the CSM and TSCO will notify the respective originating authorities, via the chain of command, of the circumstances and provide a report to include material destroyed and method of destruction.

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the right side.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen Carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (right side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call **361-961-3333**
- Handle the note as minimally as possible

If a bomb threat is received by e-mail:

- Call **361-961-3333**
- Do not delete the message

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled Words
- Incorrect Titles
- Foreign Postage
- Restrictive Notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- Follow you local guidelines
- Federal Protective Service (FPS) Police
  1-877-FPS-411 (1-877-437-7411)
- 911

BOMB THREAT CHECKLIST

Date: _____ Time: _____

Time Caller Hung up: _____ Phone number where Call Received: _____

Ask Caller:

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?
Did you place the bomb? Yes No
Why?
What is your name?

Exact Words of Threat

Information About Caller

Where is the caller located? (background and level of noise)
Estimated age:
Is voice familiar?
If so, who does it sound like?
Other points:

Caller's Voice
- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep voice
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Excited
- ☐ **Female**
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ **Male**
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background Sounds
- ☐ Animal Noises
- ☐ House Noises
- ☐ Kitchen Noises
- ☐ Street Noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long distance

Threat Language
- ☐ Incoherent
- ☐ Message read
- ☐ Taped
- ☐ Irrational
- ☐ Profane
- ☐ Well-spoken

Other Information: _____