



DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY NAPLES ITALY
PSC 817 BOX 1
FPO AE 09622-0001

NAVSUPPACTNAPLESINST 5511.6E
N3

18 FEB 2022

NAVSUPPACT NAPLES INSTRUCTION 5511.6E

From: Commanding Officer, U.S. Naval Support Activity, Naples

Subj: EMERGENCY ACTION PLAN AND EMERGENCY DESTRUCTION PLAN

Ref: (a) CMS-1A Communications Security Material System Policy and Procedures for CMS-1 Tiers 2 & 3
(b) SECNAVINST 5510.36B, Department of the Navy Information Security Program
(c) CNSSINST 4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material
(d) NAVSUPPACTNAPLESINST S3300.1 (Ser 001)

Encl: (1) Emergency Action Plan for Fire
(2) Emergency Action Plan for Natural Disaster
(3) Emergency Action Plan for Hostile Action
(4) Precautionary Destruction Priorities
(5) Complete Destruction Priority
(6) Inadvertent Disclosure Agreement
(7) Emergency Destruction Techniques
(8) Precautionary and Complete Destruction Cards
(9) Emergency Destruction Check-Off List
(10) Emergency Destruction Drill Procedures

1. Purpose. Per references (a) through (d) the Emergency Action Plan (EAP) and Emergency Destruction Plan (EDP) establishes policy for planning, training, and implementing actions to safeguard classified and cryptographic material in the event of an emergency (i.e. natural disaster or hostile action). Every effort will be made to protect classified materials while balancing the physical safety of personnel.

2. Cancellation. NAVSUPPACTNAPLESINST 5511.6D

3. Background. All classified materials including equipment, keying material, computers, tapes, Compact Disks (CDs), KSV-21 cards, documents, publications, and other classified material must be protected during emergency situations.

4. Scope. This EAP/EDP applies to all personnel assigned to U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy.

5. Policy. All Department Heads (DH) responsible for spaces that hold classified material will ensure a copy this instruction is readily available and reviewed annually. Additionally, DHs will maintain space specific emergency destruction cards in each space with classified material. All

18 FEB 2022

personnel with access to the space must be familiar with these procedures and be prepared to implement them upon direction from the Commanding Officer (CO), Executive Officer (XO), senior officer (SO) present, or the Command Duty Officer (CDO). The command security managers will schedule emergency action and destruction drills annually and divisions with communication security (COMSEC) material will hold drill on a quarterly basis.

6. Definitions.

a. Emergencies requiring execution of the EAP/EDP normally fall into two categories:

(1) Natural disaster. An emergency resulting from fire, flooding, tornado, earthquake, or hurricane. Directing actions to maintain control over the material until the emergency has passed can be a viable option.

(2) Hostile Action. An emergency resulting from enemy attack, terrorist actions, civil disturbance, mob, or riot. Assume the classified/cryptographic material is a target and direct actions to keep the material from unauthorized persons.

b. When an emergency occurs there are three courses of action possible to protect classified material:

(1) Emergency Protection. Secure and safeguard all classified material. Depending on the situation, classified material may need to be safeguarded, evacuated, relocated, or destroyed in order to ensure its protection. Classified material will be secured in General Services Administration (GSA) approved security containers when not in use. To simplify emergency destruction and or evacuation, items must be segregated according to priority and multiple items of the same priority must be stored together.

(2) Emergency Removal. If a controlled space must be evacuated, make every effort to prevent unauthorized access to the material. The EDP card, found in enclosure (8), cover required actions in the event of an emergency. Cards must be clearly marked and placed in the EAP/EDP folder. If classified material is endangered, the senior person present will immediately take measures to safeguard the classified material. Removed material must be under guard in an area where physical security can be maintained. Guards will maintain vigilance, ensuring no materials are removed from the area, and administer enclosure (6), to personnel who have been exposed to classified information without the appropriate clearance. Removal action occurs simultaneously with emergency response efforts but must not interfere with emergency response or subject personnel to unnecessary danger. Classified material can be securely stored in any of the following alternate locations:

(a) Naval Computer and Telecommunications Station (NCTS), Naples, Key Management Infrastructure Vault (KMI) (located in building 440, KMI Vault). Call DSN: 314-626-3953 for access. Combination held by KMI Vault.

18 FEB 2022

(b) NAVSUPPACT Naples N1 safe (located in building 442 room 255).
Combination held by NAVSUPPACT Naples N1 personnel.

(c) NAVSUPPACT Naples Emergency Operations safe (located in building 403 room 106.1). Combination held by NAVSUPPACT Naples N1 department.

(d) NAVSUPPACT Naples CO/XO safe (located in building 442, room 248).
Combination held by the CO/XO.

(e) NAVSUPPACT Naples Anti-terrorism Force Protection (ATFP) safe (located in building 403, room 236). Combination held by the ATFP Office personnel.

(f) NAVSUPPACT Naples Support Site SIPR Kiosk safe (located in building 2072, room C1). Combination held by NAVSUPPACT Naples/Commander SIX Fleet Security Managers.

(3) Emergency Destruction. Emergency destruction consists of two phases, precautionary and complete destruction. Complete destruction is a last resort: All reasonable efforts to secure or remove classified materials must be attempted prior to commencing complete destruction. Types of destruction are as follows:

(a) Precautionary Destruction. Designed for high-risk environments where hostile takeover is possible. Only the CO, XO, SO present, or CDO are authorized to order precautionary destruction. The priority order for precautionary destruction is listed in enclosure (4). Do not destroy any equipment, but prepare cryptographic equipment devices for destruction as noted on applicable section of enclosure (8).

(b) Complete Destruction. Complete destruction is ordered when hostile takeover is imminent or the area containing classified material must be abandoned. Destroy all remaining classified material and equipment beginning with the most sensitive. Only the CO, XO, SO present, or CDO are authorized to order complete destruction. Follow the priority listing found in enclosure (5) and the applicable portion of enclosure (8). Destruction techniques are listed in enclosure (7).

7. Action

a. Divisions. All divisions managing classified material must have EDP precautionary and complete destruction cards logically directing each step of the sequence per enclosure (8). Precautionary destruction and complete destruction cards must be distinguishable.

(1) EDP cards will be readily available to all personnel working in each space to include duty personnel.

18 FEB 2022

(2) EDP cards will include step-by-step instructions with sufficient detail so that an individual with little or no training can implement the actions. Cards should not designate names or rate/rank titles.

(3) There will be little time in an emergency to destroy classified material. EDP plans should allow for complete destruction in one hour or less.

(4) Reference (b) authorizes the senior individual present in a space containing classified materials to deviate from the established plans when circumstances warrant. Personnel safety is paramount. Maintaining an accurate record of an emergency destruction event is essential to the effective evaluation of loss and is second in importance only to the destruction itself.

b. The NAVSUPPACT Naples Command Security Manager (CSM) and Command Physical Security Officer (SECO). The NAVSUPPACT Naples CSM and SECO will function as the command destruction supervisors and will designate division/space destruction supervisor(s). Division destruction supervisors will periodically report the progress of emergency destruction actions for their respective divisions and spaces. The CSM and SECO will maintain copies of the master emergency destruction check-off list.

c. Destroyed material accountability is essential. Destruction personnel will write down the short titles, editions, equipment serial numbers, and accounting data for every item destroyed. The KMI local element custodian or CSM will provide required information to NCTS Naples KMI manager to ensure notification of proper authorities per reference (a), chapter 9. COMSEC destruction and incident reports are classified "Confidential" at a minimum and should be transmitted via secure means.

d. Once the message has been transmitted, the CO or KMI local element custodian will direct all personnel to destroy the remaining classified material (i.e. SIPRNET hard drive).

e. Personnel will report completion of this action to the destruction supervisor. The destruction supervisor will report to the CO, XO, or CDO.

8. Responsibilities

a. The CO is responsible for establishing and testing the command EAP/EDP per references (a) through (d). The CO will give two separate orders as required. "Commence Precautionary Destruction" initiates precautionary destruction and "Commence Emergency Destruction" initiates complete destruction.

b. The CSM and SECO are responsible for implementing the command EAP/EDP.

c. DHs/ Division Officers will:

18 FEB 2022

(1) Ensure their respective emergency protection plans are viable, functional, and exercised on a recurring basis.

(2) Ensure adequate tools and safety equipment IAW reference (c) are available for the safe and proper destruction of COMSEC or classified material.

(3) Ensure personnel receive scheduled training on the proper use of destruction tools and safety equipment.

d. Division officers will:

(1) Notify the CSM of required changes to the command's EAP/EDP.

(2) Maintain destruction tools and safety equipment in good working order.

(3) Hold and document emergency action and emergency destruction drills on an annual or quarterly basis as outlined in paragraph 4.

e. The CSM in cooperation with the KMI local element custodian is responsible for the overall coordination, preparation, and maintenance of the command EAP/EDP.

f. The CDO will:

(1) Issue precautionary and complete destruction orders as required in the absence of the CO, XO, or other qualified SO.

(2) Ensure overall destruction and complete the emergency destruction check off list as required.

9. Training and Drills. Emergency destruction drills will be conducted quarterly by each division holding classified material to determine effectiveness. Enclosure (10) recommends a method to conduct emergency drills without risking loss or compromise. This instruction will be reviewed and updated annually.

10. Emergency Access to Safe Combinations. A record of NAVSUPPACT Naples combinations for safes containing either COMSEC or classified material is individually packaged in an SF-700 envelope and stored in the N1 safe.

11. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records' disposition schedules located on the Department of the Navy Assistant for Administration, Directives and Records Management Division portal page

18 FEB 2022

at: <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

b. For questions concerning the management of records related to this instruction or the records' disposition schedules, please contact the local records manager or the OPNAV Records Management Program (DNS-16).

12. Review and Effective Date. Per OPNAVINST 5215.17A, NAVSUPPACT Naples will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, Navy policy, and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years unless revised or cancelled in the interim and will be reissued by the 10-year anniversary date if it still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.



J. W. STEWART

Releasability and distribution:

NAVSUPPACTNAPLESINST 5216.4DD

Lists: I and II

Electronic via NAVSUPPACT Naples website:

https://www.cnic.navy.mil/regions/cnreurafcnt/installations/nsa_naples/about/departments/administration_n1/administrative_services/instructions.html

18 FEB 2022

EMERGENCY ACTION PLAN FOR FIRE

1. All applicable personnel will familiarize themselves quarterly with the actions required to protect communication security (COMSEC) material or classified information in the event of a fire.

a. Responsibilities

(1) An individual discovering a fire will sound the alarm. Personnel assigned to the space are responsible for the initial firefighting effort.

(2) Supervisors in spaces with COMSEC are responsible for the following:

(a) Verify that the fire is reported and initial firefighting actions are taken.

(b) Provide on-the-scene protection of COMSEC and classified material during the emergency.

(c) Ensure the protection of COMSEC and classified material when outside firefighters are admitted into secure areas.

(d) Secure or remove classified material and classified COMSEC material if evacuation is directed.

(e) Assess and report probable compromise of classified material and classified COMSEC material to unauthorized persons during the emergency.

(f) Complete the inadvertent disclosure agreement contained in enclosure (6) by noting all unauthorized personnel exposed to COMSEC or classified material during firefighting actions.

(g) Complete an inventory of classified or COMSEC material and report losses or unauthorized exposure to the Key Management Infrastructure (KMI) local element custodian and the chain of command.

(h) Designate an authorized KMI local user as an alternate to execute the above actions as required.

b. Notification. In the event of an actual fire in a controlled space, the Commanding Officer, Executive Officer (XO), Command Duty Officer (CDO), Command Security Manager (CSM), and Command Physical Security Officer (SECO), and appropriate DH or Division Officer will be notified.

Enclosure (1)

18 FEB 2022

c. Procedures

(1) Each space must have a fire evacuation diagram posted or filed in an area accessible to office personnel.

(2) The senior person present must use proper judgment in implementing all portions of this plan, depending on the circumstances. Whatever actions are taken, the senior person must give utmost consideration to the safety of personnel and the security of COMSEC and classified material.

(3) Personnel assigned to non-COMSEC spaces will immediately evacuate to a safe location.

(4) Personnel in spaces with secure terminal equipment (STE) will either remove the associated KSV-21 cards and store them in a General Services Administration (GSA) approved safe or remove and maintain positive control of the KSV-21 cards until they can be properly stored. Following the casualty, an inventory must be taken.

d. Reporting

(1) After the emergency is over and re-entry into a COMSEC or classified space has been authorized, the CSM and one other authorized person will assess and report probable compromises of COMSEC material to the KMI local element custodian.

(2) In the absence of the CSM, the SECO, and the assistant CSM will appoint two personnel who are familiar with the space to conduct the investigation and ensure they submit a prompt report to the KMI local element custodian via the chain of command.

(3) The KMI local element custodian will conduct a post emergency inventory of all COMSEC material in all spaces. Any losses or unauthorized exposure will be reported to appropriate authorities per chapter 9 and chapter 10 of reference (a).

(4) When the emergency is over, the names of all firefighters and rescue personnel will be reported to the NCTS KMI Manager for debriefing if the emergency occurred in a COMSEC space.

18 FEB 2022

EMERGENCY ACTION PLAN FOR NATURAL DISASTER

1. If sufficient notification has been received that a natural disaster is imminent and relocation is required, the Commanding Officer (CO) or Executive Officer (XO) will designate an evacuation site. The following actions are required for communication security (COMSEC) users:
 - a. If time permits, return all COMSEC material and equipment to the Key Management Infrastructure (KMI) vault at Naval Computer and Telecommunications Station (NCTS), Naples, Italy, Room F201 in the C4I building. Ensure COMSEC material and equipment is handled per reference (a).
 - b. If an immediate evacuation is initiated, execute precautionary destruction card located in enclosure (8).
2. Should a disaster of this nature occur without warning, COMSEC users must follow the procedure for the protection of COMSEC material as outlined in paragraph 7b of this instruction.
3. Reporting. After the emergency condition has ended and authorization has been granted to re-enter the space, the KMI local element custodian and SECO will conduct an inventory of all COMSEC material and equipment held in the facility and report any loss or unauthorized exposure to the NCTS KMI manager per reference (a), chapter 9.

Enclosure (2)

EMERGENCY ACTION PLAN FOR HOSTILE ACTION

1. Reference (d) contains the command's physical security program, which identifies the minimum security requirements for the protection of U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy, resources. In addition to these requirements, it lists four different levels of terrorist threat conditions which may be implemented by the Commanding Officer (CO). As each stage is implemented, the following actions will be taken to minimize compromise of communication security (COMSEC) and classified material (the decision to execute complete or precautionary destruction rests with the CO or delegated authority):

a. NAVSUPPACT Naples personnel will make every effort to return all COMSEC material not required to sustain operations to the Key Management Infrastructure (KMI) vault at Naval Computer and Telecommunications Station (NCTS), Naples, Italy, Room F201 in the C4I building.

b. If the situation precludes the return of COMSEC material, destruction procedures will be followed per enclosure (8).

c. Departments and divisions holding classified material will destroy all material deemed unnecessary to sustain operations or will store it in a General Services Administration (GSA) approved container.

d. All spaces will notify the destruction supervisor when the above steps have been completed and reporting will be conducted in the same manner as described in enclosures (1) and (2).

18 FEB 2022

PRECAUTIONARY DESTRUCTION PRIORITY

1. When precautionary destruction is ordered, destroy keying material, non-essential classified manuals, and classified material.

a. Precautionary Destruction Priority List A

(1) Superseded keying material and secondary variables.

(a) TOP SECRET primary keying material.

(b) SECRET, CONFIDENTIAL, and UNCLASSIFIED primary keying material.

(2) Future (reserve on board (ROB)) keying material for use one or two months in the future.

(3) Non-essential classified material:

(a) Maintenance manuals.

(b) Operating manuals.

(c) Administrative manuals.

(d) Other classified material as designated in advance.

18 FEB 2022

COMPLETE DESTRUCTION PRIORITY

1. When complete destruction is ordered, destroy the following list of material in priority order.
2. Complete Destruction Priority List B. When sufficient personnel and facilities are available, destroy communication security (COMSEC) material in the following order:
 - a. Keying Material:
 - (1) Currently effective keying material designated CRYPTO (including key stored electronically in crypto equipment and fill devices).
 - (2) Zeroize all secure telephone (STE) keying material held in the following order: Operational Keying Material designated TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED.
 - (3) Superseded tactical operations codes classified below SECRET.
 - (4) All remaining classified keying material, authentication systems, maintenance, and unused one-time pads.
 - b. COMSEC aids:
 - (1) Complete COMSEC equipment maintenance manuals or their sensitive pages. When there is insufficient time to completely destroy these manuals, make every reasonable effort to destroy their sensitive pages.
 - (2) National, department, agency, and service general doctrinal guidance publications.
 - (3) Status documents showing the effective dates for COMSEC keying material (Supply Chain Management Review, SCMR, and all client automation, CA, messages).
 - (4) Remaining classified pages of maintenance manuals.
 - (5) Classified cryptographic and non-cryptographic operational general publications (e.g. AMSGs and NAGs).
 - (6) Cryptographic Operating Instructions (KAOs).
 - (7) Remaining classified COMSEC documents.
 - c. Equipment. Make a reasonable effort to evacuate equipment, but the immediate goal is to render cryptographic equipment unusable and un-repairable.

Enclosure (5)

NOTE: Although it is desirable to destroy jeopardized crypto-equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most field environments.

(1) Zeroize the equipment if the keying element cannot be physically withdrawn.
Example: KIV-7s, KG-175s

(2) Remove and destroy readily removable classified elements (e.g. printed-circuit boards).

(3) Destroy remaining classified elements.

NOTE: Unclassified chassis and unclassified elements need NOT be destroyed.

(4) Zeroize all loaded STEs held based on level of keying material loaded into the terminal: TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED.

NOTE: If lack of power prohibits zeroizing keying material or a loaded terminal, ensure all keying material fill devices (FD/KOVs) are physically removed from the area. In extreme emergencies, attempt to physically destroy FD/KOVs. Material can be broken or burned as much as possible to prevent unauthorized use.

3. Complete Destruction Priority List C. When sufficient personnel and facilities are available, destroy COMSEC material in the following order:

a. Keying Material:

(1) All superseded keying material designated CRYPTO except tactical operations and authentication codes classified below secret.

(2) Currently effective keying material designated CRYPTO (including key stored electronically in crypto equipment and fill devices), except unused two-holder keying material and unused one-time pads. Zeroize equipment, STE phone, and Fortezza cards at this time.

(3) TOP SECRET ROB key material marked CRYPTO becoming effective within the next 30 days that was not destroyed in precautionary destruction.

(4) Superseded tactical operations codes classified below SECRET.

(5) SECRET and CONFIDENTIAL ROB becoming effective with the next 30 days and was not destroyed in precautionary destruction.

b. Equipment. Priority Three complete destruction materials consist of:

18 FEB 2022

(1) Equipment destruction, the immediate goal is to render cryptographic equipment unusable and un-repairable.

(2) Remove and destroy readily removable classified elements.

(3) Destroy remaining classified elements.

INADVERTENT DISCLOSURE AGREEMENT

1. Information of sensitive intelligence, the source of which cannot be disclosed, has been either discussed with you or exposed to your view. This disclosure was unintentional. It is therefore necessary to acquaint you with the law on this subject and for you to execute a statement binding you to secrecy in connection with any information you may have gained from this disclosure.

2. It is impossible to over-emphasize the importance of safeguarding this intelligence. The time limit for safeguarding of such intelligence never expires. It is directed, therefore, that all reference to the existence of this information, or to words, which identify it, be strictly avoided. Transmission or revelation of this information in any manner to an unauthorized person is prohibited.

3. Although you inadvertently gained information not intended for you, your signature on the attached statement does not constitute an indoctrination or clearance for such intelligence.

a. For Subject Individual. I hereby affirm I have read and I understand the above instruction for maintaining the security of certain sensitive intelligence. I certify I will never divulge the classified information inadvertently exposed to me, and I will not reveal to any person my knowledge of the existence of such information. I understand transmission or revelation of this information in any manner to an unauthorized person is punishable under the appropriate articles of the Uniform Code of Military Justice. I further certify I will never attempt to gain unauthorized access to such information. My signature below does not constitute indoctrination or clearance but acknowledges my understanding of the above.

Affirmed Signature:

Witness Signature:

Printed Name _____

Printed Name _____

SSN _____

SSN _____

Date _____

Date _____

18 FEB 2022

EMERGENCY DESTRUCTION TECHNIQUES

1. All hands must be prepared to carry out the complete destruction of all classified materials. Maintaining the tools required to complete the destruction is necessary for all divisions with classified spaces.

a. Paper materials and publications. Paper material can be shredded, mulched, or burned. Paper shredders and disintegrators authorized for destruction of up to SECRET level classified material can be found in Emergency Operations Center (EOC) or U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy, Administration office secure rooms.

b. Paper Key Tape. Will be shredded utilizing the resources listed above.

c. Computer Hard Drives. All secret hard drives are mounted on slide mounts to expedite removal and destruction. The main goal is to damage the disk platters and misalign critical components. Use a heavy hammer or the pointed end of a fireman's axe to strike the exterior near the disk platters several times, then flip it over and strike the opposite side. Past practices to mechanically grind or chemically destroy disk platter surfaces are unnecessary.

d. Laptop Computers. Use the pointed end of a fireman's axe or heavy hammer to vigorously strike and penetrate the installed storage components. Several hits may be necessary. Do not waste time destroying the display and avoid damaging the batteries as they may pose a safety hazard.

e. Magnetic Tapes. Use a heavy hammer to break the plastic casing. Burn the tape in an open fire. Magnetic tape will clog a shredder.

f. Equipment circuit cards/PC cards/memory sticks. Destroy embedded microchips and internal connections with a heavy hammer and, if available, use metal snips or scissors to cut cards into several pieces.

g. CD/DVD/Optical Disk. Use metal snips or scissors to cut into several pieces, break in half with hands, burn in an open fire, or utilize a CD shredder located in EOC or NAVSUPPACT Naples Administration Office secure rooms.

h. STE Fortezza/KSV-21 Cards. Zeroize card following the instructions on the phone display. Strike both sides several times with a heavy hammer.

Enclosure (7)

PRECAUTIONARY AND COMPLETE DESTRUCTION CARDS

PRECAUTIONARY DESTRUCTION CARD NAVSUPPACT NAPLES ANTI-TERRORISM
FORCE PROTECTION (ATFP) OFFICE – Page 1 of 2

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key

Location: Security precinct, ATFP building 403, room 236

Material: 10 Secret Internet Protocol Router (SIPR) hard drives, one SIPR printer, one KG-175D, two secure terminal equipment units, two Government Services Administration (GSA) Approved Safes

Action required:

Step 1: Enter room 236 (requires secure door and safe access).

Step 2: Obtain hard drive sled key and network cabinet keys from ATFP Safe.

Step 3: Unlock and remove hard drives from SIPR net computers.

Step 4: Place hard drives and cases in safe (located in room 236).

Step 5: Unlock network device cabinets, Zeroize KG 175D (SIPRNET) and remove CIK.

Step 6: Place KG-175D CIK in safe (located in room 236).

Step 7: Zeroize all STEs and KSV-21 cards not required for secure coordination of emergency response.

Step 8: Store all non-essential physical classified material not designated for destruction in safe.

Step 9: Destroy all remaining non-essential physical classified material via shredder or disintegrator.

Step 10: Lock safe and room 236.

Step 11: Sign this card and annotate the short title and edition OR material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 12: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

Enclosure (8)

PRECAUTIONARY DESTRUCTION CARD NAVSUPPACT NAPLES ADMIN SECURE ROOM – Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key

Location: Admin One, Building 442, Room 255

Material: One SIPR hard drive

Action required: (see below)

Step 1: Enter room 255 (requires secure door and safe access).

Step 2: Obtain hard drive sled key from Safe Custodian.

Step 3: Unlock and remove hard drive from SIPR net computer in room 255.

Step 4: Store hard drive without case and all non-essential physical classified material not designated for destruction in safe.

Step 5: Destroy all remaining non-essential physical classified material via shredder or disintegrator.

Step 6: Lock safe and room 255.

Step 7: Sign this card and annotate material name and serial number of items destroyed if required.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 8: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

1 8 FEB 2022

PRECAUTIONARY DESTRUCTION CARD NAVSUPPACT NAPLES EMERGENCY OPERATIONS CENTER (EOC) SECURE ROOM – Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key

Location: Security precinct, Building 403, Room 106.1

Material: Two SIPR hard drives, one SIPR printer, two GSA approved Safes, one Tandberg VTC, two KSV21s, one secure terminal equipment unit

Action required: (see below)

Step 1: Enter room 106.1 (requires secure door and safe access).

Step 2: Obtain hard drive sled key from Safe Custodian.

Step 3: Unlock and remove hard drive from SIPR net computer in room 106.1.

Step 4: Store hard drive without case and all non-essential physical classified material not designated for destruction in safe.

Step 5: Zeroize all STEs, VTCs and KSV-21 cards not required for secure coordination of emergency response.

Step 6: Destroy all remaining non-essential physical classified material via shredder or disintegrator.

Step 7: Lock safe and room 106.1.

Step 8: Sign this card and annotate material name and serial number of items destroyed if required.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 9: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

PRECAUTIONARY DESTRUCTION CARD NAVSUPPACT NAPLES COMMANDING OFFICER (CO)/EXECUTIVE OFFICER (XO) OFFICE – Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key

Location: Admin One, Building 442, Room 248 and 243

Material: Two SIPR hard drives

Action required: (see below)

Step 1: Enter room 248 (requires secure door and safe access).

Step 2: Obtain hard drive sled key from Safe Custodian.

Step 3: Unlock and remove hard drives from SIPR net computers in room 248 and 243.

Step 4: Store hard drives without cases and all non-essential physical classified material not designated for destruction in safe.

Step 5: Destroy all remaining non-essential physical classified material via shredder or disintegrator.

Step 6: Lock safe and room 248.

Step 7: Sign this card and annotate material name and serial number of items destroyed if required.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 8: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

PRECAUTIONARY DESTRUCTION CARD SUPPORT SITE (SS) KIOSK– Page 1 of 2

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key

Location: GRICIGNANO SUPPORT SITE, CHAPEL building B2072, room C1

Material: Three hard drives, one KG-175G, one VTC, two secure terminal equipment units

Action required: (see below)

- Step 1: Enter room C1 (requires secure door and safe access).
- Step 2: Obtain hard drive sled key and network cabinet keys from SS Safe.
- Step 3: Unlock and remove hard drives from SIPR net computers.
- Step 4: Place hard drives and cases in safe (located in room C1).
- Step 5: Unlock 2 network device cabinets, zeroize KG 175(SIPRNET) and KIV-7(Secure VTC) and remove CIK's.
- Step 6: Place KG-175 and KIV-7 CIKS in safe (located in room C1).
- Step 7: Zeroize all STEs and KSV-21 cards not required for secure coordination of emergency response.
- Step 8: Store all non-essential physical classified material not designated for destruction in safe.
- Step 9: Destroy all remaining non-essential physical classified material via shredder or disintegrator.
- Step 10: Lock safe and room C1.
- Step 11: Sign this card and annotate the short title and edition OR material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 12: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

1 8 FEB 2022

COMPLETE DESTRUCTION CARD NAVSUPPACT NAPLES EOC – Page 1 of 2

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key, network cabinet keys, heavy hammer, and Philips screw driver

Location: Security precinct, building 403, room 132

Material: Four SIPR hard drives, one KG-175, one KIV-7, two secure terminal equipment units, two KSV-21 cards, one KG-175 Master CIK

Action required: (see below)

- Step 1: Enter room 132 (requires secure door and safe access).
- Step 2: Obtain hard drive sled key and network cabinet keys from EOC safe.
- Step 3: Unlock and remove hard drives from SIPR net computers.
- Step 4: Place hard drives and cases in safe (located in room 132).
- Step 5: Remove hard drive from sled using Philips screw driver.
- Step 6: Using hammer smash hard drive until internal platters are in many pieces.
- Step 7: Unlock two network device cabinets; remove KIV-7 and KG-175 and strike with hammer until unusable and unrepairable.
- Step 8: Remove KIV-7 CIK, KG-175D CIK, and KG-175D Master CIK from safe and strike with hammer until unusable and unrepairable.
- Step 9: Remove two KSV-21 cards from safe and strike on both sides several times with hammer.
- Step 10: Using a shredder and disintegrator destroy all classified paper and non-paper material remaining in safe.
- Step 11: Lock safe and room 132.
- Step 12: Sign this card and annotate the short title and edition or material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 13. Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

COMPLETE DESTRUCTION CARD NSA NAPLES ADMIN SECURE ROOM – Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key, Phillips screw driver, and heavy hammer

Location: Admin One, building 442, room 255

Material: 1 SIPR hard drive

Action required: (see below)

- Step 1: Enter room 255(requires secure door and safe access).
- Step 2: Obtain hard drive sled key from Safe Custodian.
- Step 3: Unlock and remove hard drive from SIPR net computer in room 255.
- Step 4: Remove hard drive from sled using Phillips screw driver.
- Step 5: Using hammer, smash hard drive until internal platters are in many places.
- Step 6: Using a shredder and disintegrator destroy all classified paper and non-paper material remaining in safe.
- Step 7: Lock safe and room 255.
- Step 8: Sign this card and annotate material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 9: Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

18 FEB 2022

COMPLETE DESTRUCTION CARD NAVSUPPACT NAPLES ATFP SECURE ROOM –
Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key, Phillips screw driver, and heavy hammer

Location: Security precinct, building 403, room 213b

Material: One SIPR hard drive

Action required: (see below)

- Step 1: Enter room 213b (requires secure door and safe access).
- Step 2: Obtain hard drive sled key from Safe Custodian.
- Step 3: Unlock and remove hard drive from SIPR net computer in room 213b.
- Step 4: Remove hard drive from sled using Phillips screw driver.
- Step 5: Using hammer, smash hard drive until internal platters are in many places.
- Step 6: Using a shredder and disintegrator destroy all classified paper and non-paper material remaining in safe.
- Step 7: Lock safe and room 213b.
- Step 8: Sign this card and annotate material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 9. Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

1 8 FEB 2022

COMPLETE DESTRUCTION CARD NAVUPPACT NAPLES CO/XO OFFICE – Page 1 of 1

Personnel required: Two personnel with secret clearance

Tools required: Hard drive case key, Phillips screw driver, and heavy hammer

Location: Admin One, building 442, room 248 and 243

Material: Two SIPR hard drives

Action required: (see below)

- Step 1: Enter room 248 (requires secure door and safe access).
- Step 2: Obtain hard drive sled key from Safe Custodian.
- Step 3: Unlock and remove hard drive from SIPR net computer in room 248 and 243.
- Step 4: Remove hard drives from sleds using Phillips screw driver.
- Step 5: Using hammer, smash hard drives until internal platters are in many places.
- Step 6: Using a shredder and disintegrator destroy all classified paper and non-paper material remaining in safe.
- Step 7: Lock safe and room 248.
- Step 8: Sign this card and annotate material name and serial number of items destroyed.

Short Title	Edition	Material Name	Serial Number

“All materials have been properly destroyed/stored as annotated on the attached list.”

Signed _____ Signed _____

Step 9. Return this card to the destruction supervisor.

SAFETY IS FIRST
NOT TO ENDANGER HUMAN LIFE

EMERGENCY DESTRUCTION CHECK-OFF LIST

1. Assumption. The CO has ordered the emergency destruction of classified material. The Command Security Manager (CSM) and Command Physical Security Officer (CPSO) present will complete this check-off list as Destruction Supervisor.

2. Action Reports

Precautionary Destruction

_____ Commanding Officer (CO) or Senior Officer (SO) present issues the following order, "Commence Precautionary Destruction".

_____ All hands involved in destruction report to their assigned destruction locations.

_____ The Emergency Destruction Plan (EDP) cards will be turned in to the destruction supervisor when precautionary destruction is complete.

_____ Emergency Operation Center (EOC) phone extension: 6635

_____ Administration Office phone extension: 5421

_____ Anti-Terrorism Force Protection (ATFP) phone extension: 5914

_____ The Electronic Key Management System (EKMS) Local Element Custodian will draft a message to the controlling authority listing the materials destroyed during precautionary destruction and provide to the Naval Computer and Telecommunications Station (NCTS), Naples, Italy, EKMS manager.

_____ The Destruction Supervisor will notify the CO once precautionary destruction is complete and users are standing by to begin the complete destruction.

Complete Destruction

_____ The CO or SO present will issue the following order, "Commence Emergency Destruction".

_____ The EKMS Local Element Custodian or the CSM will notify the NCTS EKMS manager that complete destruction is being carried out.

_____ Work centers/divisions will notify the destruction supervisor when complete destruction is finished.

_____ EOC phone extension: 6635

_____ Administration Office phone extension: 5421

_____ Anti-Terrorism Force Protection (ATFP) phone extension: 5914

_____ The EKMS Local Element Custodian will draft a message to the controlling authority listing the materials destroyed and provide to the NCTS EKMS Manager.

_____ The destruction Supervisor will report to the CO once destruction is complete.

18 FEB 2022

EMERGENCY DESTRUCTION DRILL PROCEDURES

1. To prepare for simulated destruction, follow the steps outlined in the Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP).
 - a. The senior person implementing destruction will issue destruction cards to all personnel involved.
 - b. Each person will follow the steps on the destruction card(s) noting type, method, and completeness of destruction when simulated action is complete.
 - c. After completing all steps on the card, each person report completion. The person in charge will report to the senior person implementing destruction when destruction is complete.
 - d. When all simulated destruction is complete and the drill is terminated, the senior person implementing destruction will hold a critique to discuss any recommendations/problems with the drill.
 - e. Emergency destruction drills will be conducted by all work centers holding classified materials quarterly.
 - f. The senior person implementing destruction will report the response time and any comments/problems encountered to the Command Security Manager after the drill.