ADM 1642

08/19/03

SUBJECT: CONTROL AND RELEASE OF CLASSIFIED INFORMATION AND MATERIAL

1. PURPOSE: This Directive establishes procedures regarding the control and release of classified information and material.

2. DISTRIBUTION: All Federal Air Marshal Service (FAMS) employees.

3. BACKGROUND: Under Executive Order 12958, consistent with law, directives and regulation, each agency shall establish and enforce controls to ensure that classified information and material is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

4. RESPONSIBILITY:

a. It is the responsibility of supervisors to:

1. Adhere to the policy and procedures set forth in this Directive; and,
2. Ensure that all employees under their supervision adhere to the policy and procedures set forth in this Directive.

b. It is the responsibility of employees to: Adhere to the policy and procedures set forth in this Directive.

5. POLICY:

a. A cleared FAMS employee (one who has been granted a valid security clearance) shall ensure that classified information and material under their control and custody is only disclosed to other authorized persons who themselves possess the requisite clearance level, as is necessary for the performance of tasks or services essential to the fulfillment of assigned duties.

b. The use of computer equipment for processing classified information and material is prohibited. FAMS employees should not store, process, or e-mail classified information or material on any system not explicitly approved for that purpose.

c. Classified information and material shall only be stored under conditions adequate to prevent unauthorized persons from gaining access. The requirements prescribed in Section 6., *PROCEDURES*, are the minimum acceptable security standards for the safekeeping of classified information and material.

6. PROCEDURES:

a. Storage of classified information and material: Classified information and material that is not under the personal control and observation of an authorized cleared FAMS employee shall be stored in a locked security container as follows:

1. Information and material classified as "Top Secret" or "Secret" shall be stored in a GSA approved security container, a Class A vault or a vault-type room that meets the standards established by the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS). Information and material classified as "Confidential" may be stored in the same manner as that authorized for "Top Secret" and "Secret", or it may be stored in a steel file cabinet secured by a steel bar and a three-position, GSA approved, dial-type combination padlock;

2. Protection of lock combinations for security containers, vaults, cabinets, and authorized security areas is mandatory. FAMS employees shall make every reasonable effort to minimize the number of authorized persons that have knowledge of lock combinations to such containers and areas;

3. Security containers shall bear no external markings indicating the security level of classified information and material authorized for storage in the container;

4. The names of persons having knowledge of the lock combination shall be maintained as part of the office files and records;

5. Security containers, vaults, cabinets, and authorized security areas shall be kept locked when not under the direct supervision of an authorized cleared FAMS employee entrusted with the contents;

6. Lock combinations shall be safeguarded in accordance with the highest classification of the information and material authorized for storage in the security container, vault, cabinet or authorized security area. Superseded lock combinations shall be destroyed in accordance with procedures prescribed in Section h. *Destruction*;

7. If a record is made of a lock combination the record shall be marked with the highest classification of the information or material authorized for storage in the security container, vault, cabinet or authorized security area;

8. Field Offices shall establish and maintain a system to deter and detect the unauthorized introduction or removal of classified information or material from their facility. If

the unauthorized introduction or removal of classified information or material can be reasonably foreclosed through technical means, which are encouraged, no further controls are necessary;

9. The receipt of all classified information and material shall be recorded on a log sheet and maintained as a part of the office files and records;

10. For Top Secret, Secret, and Confidential information and material, the Field Office shall maintain a record that reflects:

(A) The date of the information or material;
(B) The security classification;
(C) An unclassified description of the information or material;
(C) The date of receipt and/or transfer of custody; and
(E) Details regarding receipt and/or transfer of custody including the identity of the person involved, location involved and as appropriate the activity necessitating the transfer of custody;

11. Receipt and/or transfer of custody records for classified information and material shall be retained as part of the office files and records for two years; and,

12. Each Field Office shall conduct an annual inventory of classified information and material.

b. Safeguards during use: The following precautions shall be taken to prevent unauthorized access to classified information and material:

1. When not in use, classified documents that have been removed from storage shall be kept face down, covered and under the constant surveillance of an authorized cleared FAMS employee. The cover sheets shall be Standard Forms 703 (Top Secret), 704 (Secret), and 705 (Confidential);

2. Preliminary drafts, carbon sheets, stencils, stenographic notes, worksheets, typewriter ribbons, and other items actually containing or potentially containing classified information shall be destroyed in accordance with procedures prescribed in Section h., *Destruction*, immediately after they have served their purpose, or they shall be given the same security classification and secure handling as is appropriate for the classified information they contain; and,

3. Classified information shall only be discussed when unauthorized persons cannot overhear the discussion. Particular care should be taken when there are visitors or maintenance staff nearby. All cleared employees shall be aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or locations, or in any other way that permits interception by unauthorized individuals.

c. The L3 Secure Terminal Equipment (STE): The digital based L3 Secure Terminal Equipment (STE) is the evolutionary successor to the analog based STU-III. The STE Data Terminal provides a reliable, secure, high rate digital data modem for applications where only

data transfer (FAX, PC files, Video Teleconferencing, etc.) is required. The L3 STE instrument itself is not classified. It may be installed and used in any room in which classified conversations are permitted. Special rules apply to the security of the Fortezza Card that turns the L3 STE from a regular telephone into a secure telephone. When the Fortezza card is programmed to serve as a standard crypto-ignition key (CIK) for converting the L3 STE from a normal telephone to a secure telephone, it should be secured as follows:

1. When the CIK and the L3 STE are kept in the same room, the CIK must be secured at the highest classification level of the information that the L3 STE is authorized to transmit;
2. When not kept in the same room as the L3 STE the CIK may be secured, as would a high-value item of personal property, such as a wallet or checkbook. The CIK may be stored in a locked cabinet or desk. It may also be kept in the personal possession of the authorized holder; and,
3. If it becomes necessary to vacate the office, all classified information and material must be secured in its designated locked storage container, or left in the custody of persons cleared for access to such material.

d. Mailing and hand carrying classified information and material: The following procedures apply to mailing or hand carrying classified information and material. These procedures cover the most common methods and are intended as general guidance only and not as a substitute for official regulations:

1. TOP SECRET information and material may not be sent through the U. S. Postal Service (USPS) under any circumstances. Top Secret information and material must be hand-carried by cleared courier or transmitted by approved electronic means;
2. SECRET information and material may be transmitted by approved electronic means or delivered by USPS Registered mail or Express mail within and between the United States and its territories. When mailed, the "Waiver of Signature and Indemnity" block on the Express Mail Label 11-B may not be executed, and the use of external (street side) Express mail collection boxes is prohibited. Secret information and material may be sent through USPS Registered mail via Army, Navy, or Air Force Postal Service facilities outside the United States, provided that the classified mailing does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or is subject to any foreign inspection. Federal Express may be used to send Secret information and material for urgent, overnight delivery only;
3. CONFIDENTIAL information and material may be transmitted by approved electronic means or sent by USPS mail subject to the same mailing procedures as SECRET information and material except that Confidential information and material may also be sent by U.S. Certified mail in addition to U.S. Registered mail or Express mail; and,
4. SECRET and CONFIDENTIAL information and material must be mailed at a USPS facility. Use of street mail collection boxes is prohibited.

e. Protecting and addressing for delivery: For transport, shipping or mailing all classified information and material must be protected with both an opaque inner and an opaque outer cover. The classified item itself must first be placed in an opaque container or an opaque envelope for the purposes of the inner cover. Once protected by the inner cover the classified item must then be further protected by placing the item in a second opaque container or a second opaque envelope for the purposes of the outer cover. Classified information and material shall be marked and addressed as follows:

1. For envelopes, write the security classification in capitol letters (preferably in red ink) on both the top and bottom of the inner cover (inner opaque envelope). For containers, write the security classification in capitol letters (preferably in red ink) on the top, bottom and all four sides of the inner cover (inner opaque container);
2. Write the complete mailing address and complete return address on the top of the inner cover. The address on the inner cover must include the name of an appropriately cleared person and the notation, *To Be Opened By Addressee Only*; and,
3. Write the complete mailing address and return address on the topside of the outer cover. Do not mark on the outer cover that the envelope or container includes classified information or material. It is prohibited to send classified mail or shipments using an address on the outer cover that includes an individual addressee by name. Classified mail or shipments must be addressed on the outer cover to the Special Agent in Charge (SAIC) or other titled position within the addressee organization.

f. Receipts: A receipt identifying the classified item, the sender and the addressee should be attached to or enclosed in the inner envelope or container. The receipt itself shall contain no classified information and must be signed and returned to the sender. Receipts for classified information or material are required as follows:

1. Custody of Top Secret information and material must occur under a continuous chain of classified material receipts documenting each individual who has custody irrespective of whether or not the Top Secret information or material leaves the facility where it is stored;
2. Custody of Secret information and material only requires classified material receipts documenting each individual who has custody when the Secret information or material leaves the facility where it is stored; and,
3. Confidential information and material only requires a receipt if the sender deems it necessary, or if the Confidential information or material is being dispatched to a foreign government.

g. Hand-carrying classified information and material: When classified information or material is personally transported by cleared courier to another location by means of surface or air transportation, contingency planning must be conducted to ensure that safeguards remain in

place under all foreseeable situations or conditions that might occur while in transit. Security requirements for hand-carried classified information and material include:

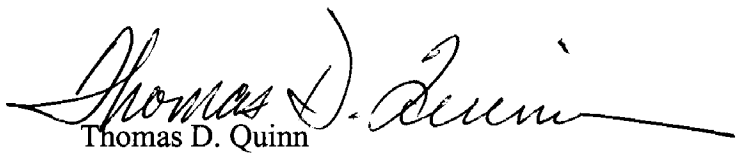
1. Hand-carried classified information and material must be wrapped, protected and addressed in accordance with procedures prescribed in Section d., Mailing and carrying classified information and material and Section e., Protecting and addressing for delivery;
2. Hand-carried classified information and material must be kept under the constant control and custody of the cleared courier and may only be delivered to the designated addressee;
3. For surface transport a briefcase may serve as the outer cover only if it is locked and approved for carrying classified material. For air travel, a locked briefcase is not permitted to serve as the outer cover for classified information and material;
4. An inventory of the hand-carried classified information and material must be prepared and one copy of the inventory should be made a part of the office files and records and the other copy given to the cleared courier; and,
5. When hand-carried classified information and material is transported by commercial or government air carrier, a written letter of authorization from the security office is required. The security officer will provide instructions and any additional requirements.

h. Destruction: Whenever classified information and material must be destroyed the following requirements must be met and procedures followed:

1. *Methods of Destruction* - Classified information and material must be destroyed either by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and hybridized disintegration equipment.) Pulpers, pulverizers, or shedders may be used only for the destruction of paper products. High wet strength paper, paper Mylar, durable-medium paper substitute, or similar water repellent type papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers. Destruction residue shall be inspected to ensure that the destroyed items cannot be reconstructed. Crosscut shredders shall be designed to produce residue particle size not exceeding 1/32 inch in width (with a 1/64 inch tolerance by 1/2 inch in length. Classified information or material in microform; that is, microfilm, microfiche, or similar high data density material may only be destroyed by burning or chemical decomposition;
2. *Witness to Destruction* - Only appropriately cleared employees shall destroy classified information and material. These individuals shall have a full understanding of their responsibilities. For destruction of TOP SECRET information and material, two persons are required. For destruction of SECRET and CONFIDENTIAL information and material, one person is required;
3. *Destruction Records* - Destruction records are required for classified information and material. The records shall notate the date of destruction, identify the items destroyed, and be signed by the individuals designated to destroy and witness the destruction. Destruction officials

shall be required to establish, through their personal knowledge, that such classified information and material was destroyed. The destruction information required may be combined with other required control records. Destruction records shall be maintained for two years; and,

4. *Classified Waste* - Classified waste shall be destroyed as soon as practical. This applies to all waste material containing classified information and material. Pending destruction, classified waste shall be safeguarded as required for the level of classified information or material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified information and material.



Thomas D. Quinn
Director, Federal Air Marshal Service