Assassination Records Review Board
SECURITY DIRECTIVE
95-1

Duties and Responsibilities

1.0 Security Officer

(a) The Executive Director of the ARRB shall be the Security Officer. It shall be the duty of the Security Officer, and such assistants as he/she may designate, to supervise the administration of this directive.

(b) The Security Officer is also responsible for the development, supervision, and administration of the Security Program, including the promulgation of policy and procedures and security directives.

(c) With respect to questions of law and policy that pertain to safeguarding National Security Information, the Security Officer shall seek advice from the Intelligence Security Oversight Office.

1.1 Employees

(a) All persons granted access to classified information in the course of their employment at the ARRB are required to safeguard that information from unauthorized disclosure. This nondisclosure obligation is imposed by statutes, regulations, access agreements, and the fiduciary relationships of the persons who are entrusted with classified information in the performance of their duties. The nondisclosure obligation continues after ARRB employment terminates. In addition, each employee having access to classified information is personally responsible for becoming familiar with

and adhering to the provisions of this directive.

(b) Employees shall be responsible for safeguarding classified information in their custody or under their control. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

(c) Employees shall be aware of the prohibition against discussing or transmitting classified information over unsecured telephones, on an unsecured computer network, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

(d) All employees with access to National Security Information are required to report to the Security Officer any close personal or social relationship with a foreign national, including foreign press representatives. This requirement does not include contacts or relationships developed within the scope of employment and known to the employee's supervisor. Any contacts with foreign nationals which result in unofficial requests for job-related information or suspicion on the part of the employee with regard to the protection of National Security Information must also be reported.

(e) All employees of the Department are to be aware of and comply with regulations concerning travel outside the continental United States. These regulations are summarized below:

> Pursuant to provisions of Director of Central Intelligence Directive 1/20 entitled "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information," ARRB personnel who have access to Sensitive Compartmented information are required to advise the Security Officer in writing, of any travel whether official or unofficial, outside of continental United States. Upon the determination of the Security Officer, it may be necessary that such personnel be provided a Defensive Security

Briefing, a formal advisory which alerts traveling personnel to the potential for harassment, provocation, or entrapment.

(f) All ARRB employees granted access to classified information in the course of their employment with the ARRB shall be required to sign a nondisclosure agreement concerning the protection of national security information and a statement that they understand and shall conform to the provisions of this directive.

(g) All employees with authorized access to Sensitive Compartmented Information shall be required to sign nondisclosure agreements containing a provision for prepublication review to assure deletion of Sensitive Compartmented Information and other classified information. Sensitive Compartmented Information is information that not only is classified for national security reasons as Top Secret, Secret , or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. The prepublication review provision will require that ARRB employees who are authorized access to Sensitive Compartmented Information submit certain material, described further in the agreement, to the ARRB or its designated successor in the U.S. Government prior to its publication to provide an opportunity for determining whether an unauthorized disclosure of Sensitive Compartmented Information or other classified information would occur as a consequence of its publication.

(h) It must be recognized at the outset that it is not possible to anticipate each and every question that may arise under these agreements. The ARRB will endeavor to respond, however, as quickly as possible to specific

inquiries by individuals concerning whether specific materials require prepublication review. Persons subject to these requirements are invited to discuss their plans for public disclosures of information that may be subject to these obligations with authorized ARRB representatives at an early stage, or as soon as circumstances indicate these policies must be considered.

1.2 Security education.

The ARRB shall establish a security education program. The program established shall be sufficient to familiarize all personnel with the provisions of this directive and to impress upon them their individual security responsibilities. The security education program shall also provide for initial, refresher, and termination briefings as required.

1.3 Oversight.

A formal review to ensure compliance with the provisions of this directive shall be conducted periodically. The audit will be performed by the Security Officer or such employees designated, in the writing, by the Security Officer.

Storage, Handling and Administrative Procedures

2.0 Storage of classified material

Classified material shall be stored in an approved container or area. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information. In the case of classified storage areas, persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

2.1 Recording storage facility data.

A record shall be maintained by the Security Officer or their designee for each vault, secure area, or container used for the storage of classified information. The record shall show its location, and the names and other appropriate identifying data of persons having knowledge of the combinations to such storage facilities. General Services Administration Optional Form 63, entitled, "Security Container Information" shall be used within the ARRB for these purposes. The OF-63 containing security combinations shall be marked with the appropriate overall classification, and shall be safeguarded and stored in accordance with the protection afforded to that classification.

2.2 Administrative aids for safeguarding classified material.

At the close of each working day, a person other than the individual locking the container, shall verify that the container is secure. The time of the check followed by the checker's initials shall be recorded. A container will not be left unattended until it has been locked by an authorized person and checked by a second person. The person locking a container is responsible for insuring that another person checks the container.

2.3 Envelopes or containers.

(a) Whenever classified information is transmitted, it shall be enclosed in two opaque sealed envelopes or similar wrappings where size permits, except as provided below.

(b) Whenever classified material is transmitted and the size of the material is not suitable for transmission in accordance with 2.2(a), it shall be

enclosed in two opaque sealed containers, such as boxes or heavy wrappings.

(c) Material used for packaging shall be of such strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to facilitate the detection of any tampering with the container. The outer wrappings shall conceal all classified characteristics.

2.4 Addressing

(a) Addresses forwarding classified information shall be specific so that couriers/messengers may easily identify the intended recipients. Use of office code numbers or such phrases in the address as "Attention: Research Department," or similar aids in expediting internal routing, in addition to the organization address is encouraged.

(b) Classified written information should be folded in such a manner that the text will not be in direct contact with the inner envelope or container. A receipt form shall be attached to or enclosed in the inner envelope container for all classified information. When written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container. A receipt listing all classified information shall be attached or enclosed. The inner envelope or container shall be marked with the highest classification of the contents.

(c) The inner envelope or container shall show the address of the receiving activity, classification, including, where appropriate, the "Restricted Data" marking, and any applicable special instructions. It shall be carefully sealed to minimize the possibility of access without leaving evidence of

tampering.

(d) An outer or single envelope or container shall show the complete and correct address of the receiving activity and the return address of the sender.

(e) An outer cover or single envelope or container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

(f) Care must be taken to ensure that classified information intended only for the United States elements of international staffs or other organizations is addressed specifically to those elements.

2.5 Receipt Systems

(a) Top Secret information shall be transmitted under a chain of receipts covering each individual who receives custody.

(b) Secret and Confidential information shall be transmitted by a receipt between activities and other authorized addressees, except that in lieu of receipts, the Executive Director may prescribe such procedures as are necessary to control effectively Secret and Confidential information.

(c) Receipts shall be provided by the transmitter of the material and the forms shall be attached to the inner envelope or cover.

(1) Receipt forms shall be unclassified and contain only such

information as is necessary to identify the material being transmitted.

(2) Receipts shall be retained for at least two years.

2.6 Accountability of Top Secret Information.

(a) Top Secret Control Officers and alternate Top Secret Control Officers shall be designated, in writing, by the Security Officer. Such officers shall be responsible for receiving, transmitting, and maintaining accountability registers for Top Secret information. They shall be selected on the basis of experience and reliability, and shall have appropriate security clearances. Further, the Security Officer shall ensure that written procedures concerning accountability of Top Secret information are promulgated.

(b) All Top Secret information received or originated with the ARRB shall be immediately registered by an appropriate Top Secret Control Officer or alternate. Such registering process shall include the recording of: The date the document was received and originated; the classification of the document; the number of copies; the title and description of the document; the disposition and date; the location of the document; and the serial number assigned to the document. For example, the 25th Top Secret document received within the ARRB during 1995 could be assigned the following Top Secret control number: ARRB--95--0025.

(c) Top Secret accountability registers shall be maintained by for all Top Secret documents received.

(d) The name and title of all individuals, including stenographic and clerical personnel, to whom information in Top Secret documents has been

disclosed, and the date of such disclosure, shall be recorded. The use of a sheet of paper permanently attached to the document concerned may serve as a disclosure record or log for these purposes. Disclosures to individuals who may have had access to containers in which Top Secret information is stored need not be recorded on disclosure records.

2.7 Accountability of Secret and Confidential Information.

The Security Officer is responsible for ensuring that accountability procedures for Secret and Confidential information are established. Such procedures shall be written and shall pertain to Secret and Confidential information originated or received by the ARRB, and disposed of by the the ARRB by transfer of custody or destruction. At a minimum, such procedures shall provide for the identification of the document.

2.8 Accountability of reproduced documents.

Reproduced copies of Top Secret, Secret and Confidential documents are subject to the same accountability and controls as the original documents.

2.9 Reproduction of classified material.

(a) Reproduction of classified material shall be held to the minimum consistent with operational requirements.

(b) Classified reproduction shall be accomplished by authorized employees knowledgeable of the procedures for classified reproduction.

(c) Reproduced copies of classified documents shall be subject to the same protection as the original documents.

(d) All reproductions of classified material shall be conspicuously marked with the same classification markings and any special warning notices as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

2.10 Disposal of classified documents.
Classified documents are to be disposed of by approved methods only.

2.11 Emergency planning.
The ARRB shall have current plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action.

Security Violations and Administrative Sanctions

3.0 Violations subject to sanctions.
(a) Officers and employees of the ARRB are subject to appropriate administrative sanctions if they:

(1) Knowingly, willfully or negligently and without authorization disclose to unauthorized persons information classified under Executive Order 12958 or prior orders or compromise classified information through negligence.

(2) Knowingly and willfully violate any other provision of Executive Order 12958, any implementing directives, or this directive.

(b) Sanctions include but are not limited to warning notices, reprimands, suspension or termination of security clearance, and as permitted by law, suspension without pay, forfeiture of pay, removal or dismissal.

3.1 Reporting securing violations.
Any person subject to this directive who suspects or has knowledge of a

violation pursuant to 3.0 (including the known or suspected loss or compromise of National Security Information) shall promptly report and confirm in writing the circumstances. If the loss itself is classifiable, secure telecommunications must be used for the initial report. The loss must be confirmed in writing to the Security Officer of the agency concerned or to that official's appropriate Security Programs Manager or representative. The Security Officer shall take the following action forthwith:

(a) Prompt notification of the violation to the origination office and to any interested department or agency, if appropriate.

(b) The submission of a written report. Such report shall include the date the violation occurred, if known; the date of the discovery of the violation; the specific identification of the information involved in the violation; the national classification or any caveats regarding the information involved; the probability of loss or compromise; an assessment of the damage incurred from a national security standpoint; corrective measures taken; the person(s) responsible for the violation; and recommended administrative, disciplinary or legal action which should be taken. The written report should be submitted no later than ten working days after the discovery of the violation.

(c) The Security Officer will promptly notify the Director of the Information Security Oversight Office of any violations.

3.2 Corrective action.

The Security Officer shall ensure that appropriate and prompt corrective action is taken whenever a violation of 3.0 occurs.

3.3 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified documents and material such as failure to show classification authority, failure to apply internal classification markings and incorrect computation of dates for declassification, or other repeated disregard of requirements of this directive that are determined not to constitute a violation under **3.0** may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate by the Executive Director.