SOUTHWEST REGION
AND
SOUTHWEST FISHERIES SCIENCE CENTER
DATA CONFIDENTIALITY HANDBOOK

by

Svein Fougner
Southwest Region
National Marine Fisheries Service, NOAA
Long Beach, California 90802
and
Atilio Coan
Southwest Fisheries Science Center
National Marine Fisheries Service, NOAA
La Jolla, Califirnia 92038

Prepared in accordance with NOAA Administrative Order 216

August 1996

SOUTHWEST REGION

AND

SOUTHWEST FISHERIES SCIENCE CENTER

DATA CONFIDENTIALITY HANDBOOK

TABLE OF CONTENTS

SOUTHWEST REGION/SCIENCE CENTER DATA CONFIDENTIALITY HANDBOOK

AUGUST 1996

This handbook describes policies and procedures for protecting the confidentiality of data submitted to, collected by, or in the possession of the Southwest Region and Southwest Fisheries Science Center, as authorized or required by NOAA Administrative Order 216-100 and regulations published at 50 CFR Part 600, Subpart E (Appendix I and II, respectively), which carry out the laws establishing confidentiality requirements. The laws and regulations regarding collection, use and disclosure of confidential fisheries data are very restrictive, and the penalties for unauthorized disclosure or release of confidential data are serious. The handbook is intended to inform Region and Center staff of their obligations for maintaining the confidentiality of data possessed by NMFS and of the penalties if confidentiality is not maintained. The handbook covers all confidential data, in any form and from any source, received, collected, maintained, or used by NMFS.

The handbook does not deal with physical protection of Automated Data Processing (ADP) equipment facilities, data files, and supporting utilities; protection of data electronically communicated between and among computer centers and remote terminal locations; or hardware and software safeguard. These subjects are addressed in the Department of Commerce ADP Security Manual. Responsibility for these matters rests with the ADP managers of the Region and Center.

As used in this handbook:

Aggregate or summary form means data structured so that the identity of the submitter cannot be determined either from the present release of the data or in combination with other releases.

Agreement refers to cooperative agreements, contracts, or other binding forms of mutual commitment under a stated set of conditions made to achieve a specific objective with respect to maintaining confidential fisheries data.

Authorized use is that specific use authorized under the governing statute, regulation, order, contract or agreement.

Authorized user is any person who (a) has the need to collect or use confidential data in the performance of an official activity; (b) has read NOAA Administrative Order 216-100; and (c) has signed a statement of nondisclosure affirming the user's understanding of NMFS obligations with respect to confidential data and the penalties for unauthorized use and disclosure.

Center means the Southwest Fisheries Science Center facilities in La Jolla, Pacific Grove, Monterey, or Honolulu.

Confidential data means data that are identifiable with any person, that reveal the business practices of an individual, and that are prohibited by law from being disclosed to the public. The release of these data could place the supplier or subject of the data at a competitive disadvantage and could result in adverse impacts on that person's business.

Data refers to information used as a basis for reasoning, discussion, compilation, or calculation that a person may submit, either voluntarily or as required by statute or regulation.

Person means any individual (whether or not a citizen or national of the United States), any corporation, partnership, association, or other entity (whether or not organized or existing under

the laws of any State), or any Federal, State, local, or foreign government or any entity of such governments, including Regional Fishery Management Councils (Councils).

Region means the Southwest Regional offices in Long Beach, Santa Rosa, Honolulu, and Pago Pago.

State employee means any member of a State agency responsible for developing and monitoring the State's marine fisheries program or Marine Mammal Protection Act (MMPA) program.

Only individuals are designated "authorized users" of confidential data. Access is not provided to offices or organizations.

Confidential data shall only be disclosed to the public if required by the Freedom of Information Act (FOIA),

5 U.S.C. 552, the Privacy Act, 5 U.S.C. 552a, or by court order.

Disclosure of data pursuant to a subpoena issued by an agency of competent jurisdiction is a lawful disclosure. However, disclosure pursuant to a subpoena must be approved by NOAA General Counsel.

Individual identifiers shall be retained with data, unless the permanent deletion is consistent with the needs of NMFS and good scientific practice (See Section 4.06).

A notice is required on all report forms that request data. The notice must comply with 5 U.S.C. 552a(e)(3) and Paperwork Reduction Act requirements in NAO 216-8, Information Collections and Requirements Needing Office of Management and Budget Clearance. (See E.O. 12600 of June 23, 1987, for additional information regarding the rights of submitters to designate commercial confidential data at the time of submission.)

a. Southwest Regional Director and Science Director

The Regional Director has the overall responsibility to maintain the confidentiality of all data collected, maintained, and disclosed within and by the Region and Center.

The Regional Director and Science Director will designate Data Confidentiality Coordinators in their respective units whose responsibility it is to collaborate to ensure consistent application of confidentiality standards in the Region and the Center.

The Regional Director will determine whether a contractor is to be provided with access to confidential data.

The Regional Director may enter into agreements on behalf of NMFS with States, educational institutions, and other contractors for data collection, management, and use of confidential data consistent with the requirements of NOAA Administrative Order 216-100. Any such agreements shall be cleared by the Southwest NOAA General Counsel or the Department of Commerce, as appropriate.

b. Data Confidentiality Coordinators

The Coordinators will maintain and continually update a list of authorized users of confidential data in the Region and Center, respectively, and will exchange these lists.

The Coordinators will maintain a Central Registry containing the names and other data pertaining to persons who handle confidential data and whose need-to-know has been established, and who have signed the "Standard Statement of Nondisclosure" (see Appendix I). The nondisclosure statement will be signed by all persons who collect or access confidential

data. The Central Registry is controlled as a confidential document. Information contained in it may be revealed only to persons whose names are currently on the Central Registry. The Central Registry will be consulted by designated staff whenever it becomes necessary to determine whether a person has a need-to-know that warrants access to confidential data. Authorized persons may consult the Central Registry by contacting the appropriate Coordinator in person or by telephone.

The Coordinators will develop a catalog/inventory system of all confidential data received including: the type of source document; the authority under which each item of data was collected or obtained; any statutory or regulatory restriction(s) which may apply; and routing from the time of receipt until final disposition.

The Coordinators will develop an appropriate coding system for each set of confidential data so that access to data that identify, or could be used to identify, the person or business of the submitter is controlled by the use of one or more coding system(s). Lists that contain the codes shall be kept secure.

The Coordinators will provide a report annually to the Region and Center Directors concerning this Handbook and recommend any changes needed to be made to ensure its effectiveness and conformance with current laws, NOAA administrative requirements and NMFS regulations.

c. Managers and Supervisors

Managers and supervisors will ensure that staff handling confidential data receive and read the handbook and understand the requirements of NOAA Administrative Order 216-100.

Managers and supervisors, working with the Coordinators, will determine which staff should be designated authorized users of confidential data for specific purposes.

Managers and supervisors shall ensure that any of their staff departing their unit has certified that all confidential data which the employee possessed have been retained within the Region or Center.

d. Individual Staff

Each person needing to be designated an authorized user will receive a copy of this handbook, read NOAA Administrative Order 216-100, and sign a nondisclosure statement acknowledging the obligation to maintain data confidentiality and the penalties for unauthorized disclosure.

New staff members will be provided with a copy of this handbook as they assume their duties. With the advice of the new staff supervisor, a determination shall be made whether the new staff person should have access to confidential data. If so, he/she shall sign a nondisclosure form before being designated an authorized user.

Each authorized user will be issued a unique Access Number at the time of completion of the Statement of Nondisclosure. This Access Number will be confidential, and will be used as identification when making telephone inquiries. The Access Number will not be revealed to others, including other authorized users.

All Region and Center staff members collecting confidential data will be required to sign a nondisclosure statement acknowledging their responsibilities to maintain data confidentiality and the penalties for unauthorized disclosure of data.

Any State agency staff member collecting confidential data on

behalf of NMFS under a data agreement shall sign and provide to the Regional Director either a NMFS nondisclosure form, or a statement at least as protective as the NMFS form, acknowledging the requirements of Federal laws and policies and the Federal penalties for unauthorized disclosure.

Staff members collecting confidential data must maintain all documents containing confidential data in secure facilities, and may not disclose confidential data, whether recorded or not, to anyone not authorized to receive and handle such data.

Each contractor employee collecting or processing confidential data on behalf of the Regional Director will be required to read, date, and sign a statement of nondisclosure, that affirms the employee's understanding of NMFS obligations with respect to confidential data and the penalties for unauthorized use and disclosure of the data. Upon signature, the employee's name will be placed on record as an "authorized user," and the employee will be issued certification.

Data collected by a contractor must be transferred in a timely manner to authorized Federal employees; no copies of these data may be retained by the contractor. NMFS may permit contractors to retain aggregated data. A data return clause shall be included in the agreement. All procedures applicable to Federal employees must be followed by contractor employees collecting data with Federal authority.

a. NMFS Staff. Region and Center staff members who are designated authorized users and who have signed nondisclosure forms will be provided with access to the data consistent with their needs.

b. State staff. Staff members of a State with a data exchange agreement with the Southwest Region who have been found to need access to NMFS confidential data will be provided with such access provided they have signed NMFS nondisclosure statements, or another form or statement at least as protective as the NMFS form, acknowledging Federal data confidentiality requirements and Federal penalties for unauthorized disclosure.

In cases in which a State has entered into an agreement with another State(s), the Southwest Region will facilitate transfer or exchange of State-collected data in its possession if:

(1) NMFS has written authorization for data transfer from the head of the collecting State agency; and

(2) the collecting State has provided NMFS a list of authorized users in the recipient State(s); and

(3) the collecting State agrees to hold the United States Government harmless for any suit that may arise from the misuse of the data.

c. Council staff and members. Staff and members of a Regional Fishery Management Council may be designated authorized users and be provided access to such data, provided that (1) they have signed nondisclosure forms and (2) the Council's procedures for ensuring the confidentiality of data have been furnished to the Regional Director in the year in which access is provided. However, data submitted in accordance with a fishery management plan will be provided to a Council member only after determining, under 50 CFR 603.5(d), that the member will not gain personal or competitive advantage from access to the data and that the suppliers of the data will not be placed at a competitive disadvantage by public disclosure of the data at Council meetings or hearings.

d. Contractors

Pursuant to an agreement with NMFS, a NMFS contractor (including universities, Sea Grant investigators, etc.) may be granted "authorized user" status consistent with this Order if the use furthers the mission of NMFS.

The Regional Director will notify the contractor of his/her decision on access in writing within 30 calendar days after receipt of a request.

Contingent upon approval, the contractor will be provided with details regarding conditions of data access, any costs involved, formats, timing, and security procedures. If the request is denied, the reason(s) for denial will be given by the NMFS office involved. The denial will not preclude NMFS consideration of future requests from the contractor.

If access is granted, language in the agreement specifically dealing with confidentiality of data will be required. The language shall include all of the relevant portions of NOAA Administrative Order 216-100 and shall prohibit the further disclosure of the data. No data may be retained beyond the termination date of the agreement; and any disclosure of data derived from the accessed confidential data must be approved by NMFS.

The Regional Director shall reserve in all agreements a right of prior review of any report or other product based on or derived from confidential data to ensure protection against unauthorized inadvertent release of confidential data.

The Privacy Act allows for data to be released back to the submitter upon receipt and verification of a written request stating the data required.

Definitions

Maintenance is defined as the procedures required to keep confidential data secure from the time the source documents are received by NMFS to their ultimate disposition, regardless of format. (See National Institute of Standards and Technology "Computer Security Publications, List 91" for guidance.)

A Manual Document is any storage medium on which is recorded alphabetic, numeric and/or special characters in a form in which such characters may be read by the human eye. Examples of manual documents are (1) printed forms or notebooks with handwritten or typed entries, (2) punched cards and punched paper tape (whether interpreted or not), (3) graphs, maps, charts, tables and listings (whether prepared by hand, type-written, word processor, computer or other device), and (4) any photographic or other reproduction, facsimile or extract thereof.

A Non-Manual Document is any storage medium that contains data in a form such that the characters or character representations cannot be read by the human eye. Examples are magnetic and electronic storage media for data that are digitally encoded or in analog form.

Maintenance Procedures

a. Employees are required to be knowledgeable of the security procedures for handling confidential data in this handbook and the consequences of unauthorized removal or disclosure.

b. The permanent deletion of individual identifiers from a database shall be addressed on a case-by-case basis. Identifiers may only be deleted after:

(1) Future uses of data have thoroughly been evaluated, e.g., the need for individual landings records for allocating shares under an individual transferable quota program;

(2) Consultation with the agency(s) that is collecting data (if other than NMFS), the relevant Council(s), and the NMFS Senior Scientist; and

(3) Concurrence by the Assistant Administrator has been received prior to deletion.

c. Marking. Manual documents will be conspicuously marked with the words, "FISHERIES CONFIDENTIAL" as soon as statutory confidential data are recorded on them. Whenever practicable, the marking will be in letters not less than one-half inch in height, and will be placed at the top and bottom center of every page, in red ink. Small documents that are handled in large numbers (such as punched cards and printed forms) may be placed in appropriate containers that have covers, flaps or lids, and the protective marking may be placed conspicuously on the outside of the container. Protective markings, rubber stamps on which they are embossed, and documents on which they appear will be protected from viewing by unauthorized persons. Documents containing both confidential and nonconfidential data will bear on each page the protective marking of the most sensitive data on that page.

d. Shipping and Mailing. Confidential data may be shipped or mailed by any conventional medium. Ordinary mail, Parcel Post, Air Express, United Parcel Service and similar media are all acceptable. Couriers which are not authorized access to the material may be used, as long as the materials are securely sealed in such a manner as to make undiscovered tampering unlikely. All confidential data will be double-wrapped or double-enveloped, with the full address of the recipient on both the inner and outer wrapping or envelope. The inner wrapping or envelope will be clearly marked in red ink with the protective marking. The protective marking will not appear on the outside of the package, nor will it be visible through the outer wrapper or envelope. These procedures apply to inter-office delivery of confidential data.

e. Inter-office Transfer. A common security violation is for authorized users to carry confidential data through the hallways with the protective marking exposed. The proper security precaution is to place it in an envelope or fold it in such a way that the marking is not seen by others.

f. Reproduction. Copies of documents containing confidential data must be kept to the minimum number required for efficient operations. As a general rule, only the originator of a document should be permitted to make a copy or copies of it in whole or in part. The only exception to this is when it is clearly imprinted, as in the case where data are incorporated into a digital data file. Special written arrangements concerning reproduction will be made when manual documents are provided to persons outside NMFS.

g. Storage. Confidential data will be protected continuously from unauthorized knowledge, viewing or access. A common breach of security is to fail to cover confidential data when an unauthorized person enters the room. This can be accomplished in an unobtrusive manner so as not to bring embarrassment to the visitor. Another common error is to discuss confidential matters in public areas or over the telephone within a possible hearing distance of unauthorized persons. When confidential documents are not in use they will be placed in a heavy, lockable container (file cabinet, locker, safe or desk) and secured by locking the container. Such documents should never be allowed to remain on a desk top or in any unsecured location unguarded for any length of time. The lock may be of the built-in key type, or may be a padlock or a three-position, dial-type combination lock.

Confidential documents must not be stored in the same drawer with documents that do not contain confidential data. Under no circumstances will confidential documents be stored in any container to which unauthorized persons have access.

h. Disposition/Destruction. Confidential data are exempt from automatic decontrol. That is, there is not a prescribed period of years beyond which FISHERIES CONFIDENTIAL data are releasable to the general public or to other persons who are not registered as authorized users at that future time. Confidential data that are no longer needed will be destroyed by any appropriate means that will insure their confidentiality.

Documents containing confidential data on one side will not be recycled as scratch pads or for other uses. Documents bearing protective markings should never be placed in trash receptacles for routine disposal.

i. Log Books. A record or log will be maintained in each operating area where confidential data are received or dispatched. The log will contain a descriptive title of each confidential document received or dispatched, the date and time of the action, the number of pages or individual items involved, and the number of copies. The log will also show from whom each document was received or to whom it was dispatched. Logs will be filed in a secure place in a manner similar to that used for confidential data. They may be destroyed after four years.

j. Safeguarding of Non-Manual Documents.

(1) The physical safeguarding rules for storage devices bearing digital or analog representations of confidential data (such as magnetic tapes, discs, floppy discs, cartridges and magnetic cards) are the same as those for manual documents described above.

(2) Procedures for controlling access to, and safeguarding of, confidential data while the data are stored on the aforementioned devices is covered in the Department of Commerce ADP Security Manual. Implementation of such procedures is the responsibility of each ADP facility manager.

Employees are prohibited by Department of Commerce employee conduct regulations (15 CFR part 0) and by ethics regulations applicable to the Executive Branch (5 CFR 2635.703) from using nonpublic information subject to this Order for personal gain, whether or not there is a disclosure to a third party.

Persons who make unauthorized disclosure of confidential data may be subject to civil penalties or criminal prosecution under several statutes as listed in the Administrative Order. Persons may be subject to disciplinary action, including removal, for failure to comply with the Administrative Order. Prohibited activities include, but are not limited to, unlawful disclosure or use of the data, and failure to comply with implementing regulations or statutory prohibitions relating to the collection, maintenance, use and disclosure of data covered by this Handbook.