NIH Policy Manual

1440 - Dissemination of Security and Intelligence-Related Information

Issuing Office: OD/OM/ORS/SER/DP **Phone:** (301) 496-2387

Approving Official(s): DDM

Release Date: 10/22/2009 ?

Transmittal Notice

1. **Explanation of Material Transmitted:**
   This chapter establishes policy and describes procedures for handling the dissemination of security related information to the National Institutes of Health (NIH) community. It is being revised at this time to: a.) incorporate plain language requirements b.) in compliance with NIH Manual 1710 requirement to update manual issuances every 5 years, and c.) to reflect organizational changes resulting in the delayering of the Office of Research Services (ORS).
2. **Filing Instructions:**
   Remove: NIH Manual Chapter 1440 dated 04/30/00
   Insert: NIH Manual Chapter 1440 dated 10/22/09

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Manual System, Contact the Office of Management Assessment, OM, on 301-496-4606.
- Online information, enter this URL : http://oma.od.nih.gov/manualchapters/

A. Purpose

This chapter explains the procedures necessary to disseminate security-related and intelligence-related information of interest and/or importance to the National Institutes of Health (NIH) community.

B. Background

Security-related information and intelligence-related information is often received by NIH employees. When received from unauthorized sources, this information is frequently found to be inaccurate or misleading. The dissemination of false or inaccurate information could result in injury, death, or civil litigation and/or adversely impact ongoing security planning and

resources. This policy applies to information received from within NIH as well as outside sources. This chapter applies to all NIH employees, contractors, affiliates (fellows, guest researchers, special volunteers), visitors, patients and other staff.

C. Policy

All persons must not engage in any conduct detrimental to the Government and must avoid conflicts of private interests with public duties and responsibilities. The Chief, Division of Police (DP) is responsible for gathering/receiving, reviewing all intelligence related information, determining its accuracy and relevancy, and distributing intelligence to the appropriate NIH officials and/or others.

D. References

1. Records retention is subject to NIH Manual 1743, "Keeping and Destroying Records," Appendix 1, NIH Records Control Schedule
2. NIH Delegation of Authority #08 entitled "Control of Violations of Law at Certain NIH Facilities": http://delegations.od.nih.gov/DOADetails.aspx?id=1608

E. Definitions

1. **Security Related Information** - Information *presented by* Security and Emergency Response and/or its security related components (Division of Police [DP], Division of Physical Security Management [DPSM], Division of Personnel Security and Access Control [DPSAC], and the Division of Emergency Preparedness and Coordination [DEPC]) regarding the safety and protection of life and property.
2. **Intelligence Related Information** - Information *gathered/received and analyzed* by the DP to determine its accuracy, relevancy, and need for distribution regarding the safety and protection of life and property. Examples include personal safety alerts, notices of criminal or suspected criminal activities, and announcements of demonstrations or other civil disturbances.
3. **Security and Emergency Response, ORS** - Security and Emergency Response (SER) services support the NIH's biomedical research goal, by providing a safe work environment for the NIH employees, contractors, affiliates, visitors, research and facilities. The services within SER are:
   Division of Police (**DP**)
   Division of Emergency Preparedness and Coordination (**DEPC**)
   Division of the Fire Marshal (**DFM**)
   Division of Fire and Rescue Services (**DFRS**)
   Division of Physical Security Management (**DPSM**)
   Division of Personnel Security and Access Control (**DPSAC**)

F. Responsibilities

1. The Director, NIH has delegated authority for the protection of NIH facilities and grounds to the Associate Director for Research Services (ADRS) and the Associate Director, SER.
2. Division responsibilities:

    a. The SER service cluster is assigned primary responsibility for the development, administration, and control of comprehensive security and protection programs to safeguard NIH personnel and property.
    b. The SER, DP, DEPC, DFM, DFRS, DPSM and DPSAC are responsible for presenting all security-related information pertaining to their respective areas of responsibility.
    c. Division of Police (DP):

        (1) Intelligence gathering:

            (a) The DP is responsible for receiving, analyzing, and distributing intelligence information in a timely fashion to the NIH Executive Officers and/or appropriate NIH program personnel affected by its content.

            (b) The DP develops intelligence through ongoing information gathering and sharing with local and Federal law enforcement agencies and professional groups including the Federal Bureau of Investigation (FBI), Montgomery County Police, United States Park Police, and others.

    d. Division of Emergency Preparedness and Coordination (DEPC):

        (1) Presents all security related information to the appropriate senior NIH personnel, pertaining to DEPC's respective areas of responsibility.

    e. Division of the Fire Marshall (DFM):

        (1) Presents all security related information to the appropriate senior NIH personnel, pertaining to DFM's respective areas of responsibility.

    f. Division of Fire and Rescue Services (DFRS):

        (1) Presents all security related information to the appropriate senior NIH personnel, pertaining to DFRS' respective areas of responsibility.

    g. Division of Physical Security Management (DPSM):

        (1) Presents all security related information to the appropriate senior NIH personnel, pertaining to DPSM's respective areas of responsibility.

h. Division of Personnel Security and Access Control (DPSAC):

(1) Presents all security related information to the appropriate senior NIH personnel, pertaining to DPSAC's respective areas of responsibility.

3. All NIH employees, contractors, affiliates and other staff are responsible for complying with the policy and procedures outlined in this manual for the proper safeguarding and control of security-related and intelligence-related information.

G. Procedures

1. Intelligence information affecting the NIH community, including security/personal safety alerts, warnings of criminal or suspected criminal activities, announcements of demonstrations or other activities affecting the safety and security of the NIH campus or NIH employees, etc., must be submitted immediately and solely to DP by contacting the Chief, DP (Chief of Police) as follows:

a. Phone: 301-496-5685
b. Fax: 301-402-0394
c. Chief of Police

Building 31, Room B3B17
31 Center Drive, MSC 2012
Bethesda, MD 20892-2012
hintoal@ors.od.nih.gov

H. Records Retention and Disposal

All records (e-mail and non-e-mail) pertaining to this chapter must be retained and disposed of under the authority of NIH Manual 1743, "Keeping and Destroying Records" Appendix 1, NIH Records Control Schedule, Section 1300-C. Protection and Security (all items that apply) and Section 2300-730. Suitability, Security and Conduct (all items that apply).

NIH e-mail messages: NIH e-mail messages (messages, including attachments, that are created on the NIH computer systems or transmitted over NIH networks) that are evidence of the activities of the agency or have informational value are considered Federal records. These records must be maintained in accordance with current NIH Records Management guidelines. Contact your IC Records Officer for additional information.

All e-mail messages are considered Government property, and if requested for a legitimate Government purpose, must be provided to the requester. Employees'supervisors, NIH staff conducting official reviews or investigations, and the Office of Inspector General may request access to/or copies of the e-mail messages.

E-mail messages must also be provided to the Congressional oversight committees, if requested, and are subject to the Freedom of Information Act requests. Since most e-mail systems have back-up files that are retained for significant periods of time, e-mail messages and attachments are likely to be retrievable from a back-up file after they have been deleted from an individual's computer. The back-up files are subject to the same requests as the original messages.

I. Internal Controls

The purpose of this chapter is to provide guidance to NIH personnel.

1. **Office Responsible for Reviewing Internal Controls Relative to this Chapter:** Through this manual issuance, the Division of Police, ORS is responsible for ensuring that internal controls are implemented and working.
2. **Frequency of Review:** Annually
3. **Method of Review:** The Division of Police will maintain oversight and ensure compliance with this policy by assessing documentation obtained through routine operations and interaction with the population on the NIH campus.
4. **Review Reports:** The Chief of Police reviews all reports. Issues of special concern will be brought immediately to the attention of the Associate Director SER; Associate Director for Research Services (ADRS) and the Deputy Director for Management, (DDM).