NIH POLICY MANUAL

1440 DISSEMINATION OF SECURITY-RELATED INFORMATION
Issuing Office: ORS/DPS 496-6893
Release Date: 4/30/00

---

1. **Explanation of Material Transmitted:** This chapter establishes policy and describes the procedures for handling the dissemination of security-related information to the NIH community.

2. **Material Superseded:** N/A

3. **Filing Instructions:**

   Remove: N/A

   Insert: NIH Manual Chapter 1440 dated 4/30/00

   NOTE: This and future Manual Issuances prepared by the Office of Research Services, Division of Public Safety, will be issued in the 1400 series.

4. **Distribution:** NIH Manual Mailing Keys F-401 and F-402

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Manual Mailing Keys, contact the Division of Support Services, ORS, on 496-4808.
- NIH Manual System, contact the Office of Management Assessment, OA, on 496-2832.
- Online information, enter this URL:

  http://www3.od.nih.gov/oma/manualchapters/

NIH MANUAL 1440
DATE: 4/30/00
ISSUING OFFICE: ORS/DPS 496-6893

DISSEMINATION OF SECURITY-RELATED INFORMATION

Table of Contents

DISSEMINATION OF SECURITY-RELATED INFORMATION

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

B. BACKGROUND: Security-related information, warnings, or instructions are often received by NIH employees. Frequently this information is 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.

C. REFERENCES:

NIH Manual Chapter 1130 General Administration No. 8, *Control of Violations of Law at Certain NIH Facilities*

D. DEFINITIONS:

Security-related information - Information which affects 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. The information may be sent to employees in the form of letters, memoranda, or e-mail messages.

E. 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 Director, Division of Public Safety, Office of Research Services (ORS), in NIH Manual Chapter 1130 General Administration No. 8, *Control of Violations of Law at Certain NIH Facilities.*
2. The Division of Public Safety, ORS exercises

exclusive jurisdiction over law enforcement on the NIH campus and is assigned primary responsibility for the development, administration, and control of comprehensive security and protection programs to safeguard NIH personnel and property.

3. The Director, DPS is responsible for receiving, certifying, and disseminating all security-related information pertaining to the NIH. Through ongoing intelligence 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, DPS has the resources for receiving information critical to the security of NIH and distributing this information in a timely fashion to the NIH Executive Officers and/or appropriate NIH program personnel affected by its content.

4. NIH employees are responsible for complying with the policy and procedures outlined in this manual for the proper safeguarding and control of security-related information.

F. POLICY: The Director, DPS is responsible for reviewing all security-related information, determining its accuracy and relevancy, and distributing to the appropriate NIH officials and/or others.

G. PROCEDURES FOR FORWARDING SECURITY-RELATED INFORMATION:

Security-related 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 DPS by contacting the Director, DPS as follows:

By phone: 301-496-6893

DISSEMINATION OF SECURITY-RELATED INFORMATION

By fax: 301-402-0394
By memo: Director, Division of Public Safety
National Institutes of Health
Building 31, Room B3B12
31 Center Drive, MSC 2012
Bethesda, MD 20892-2012

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," Part 1, section 1300.

NIH e-mail messages. NIH e-mail messages (messages, including attachments, that are created on 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 the Inspector General may request access to or copies of the e-mail messages.

E-mail messages must also be provided to Congressional committees if requested and are subject to 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. MANAGEMENT CONTROLS: The purpose of this manual issuance

is to establish the NIH policy and describe the system for disseminating security-related information to the NIH community.

1. Office Responsible for Reviewing Management Controls Relative to this Chapter (Issuing Office): Through this manual issuance, the Division of Public Safety (DPS), Office of Research Services (ORS) is responsible for
the method used to ensure that management controls are implemented and working.

2. Frequency of Review: Ongoing review.

3. Method of Review: The DPS will maintain oversight and ensure compliance with this policy through a myriad of resources, e.g., complaints received from NIH employees, Administrative Officers, and/or Executive Officers; reports of security information disseminated to the NIH community without prior authorization from DPS; police reports; etc. If DPS determines that NIH employees are not following this policy, DPS will ensure that the appropriate IC officials are notified and that the issue is resolved.

4. Review reports are sent to: Director, DPS; Associate Director for Research Services; and Deputy Director for Management, NIH. Issues of special concern will be brought immediately to the attention of the Associate Director for Research Services.