NATIONAL WEATHER SERVICE INSTRUCTION 30-5101
October 28, 2008

Operations Division
Physical Security NWSPD 30-51
FACILITIES PHYSICAL SECURITY

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W/OPS15 (M. Ed Awni) **Certified by:** W/OPS1 (M. Paese)
Type of Issuance: Routine.

SUMMARY OF REVISIONS: This directive supersedes NWSI 30-5101, dated November 7, 2002 and includes the following changes:

Subsection 4.1, added sentence on Level I security rating for Weather Service Offices

Subsection 4.2, added administrative procedures for laptop computers.

Subsection 5.1.c and 5.2.c, added tasking to include physical security deficiencies in the Region's annual work plan using reporting mechanisms in the Engineering Management Reporting System to document/record physical security deficiencies. Also included provisions to classify work as deferred, if funding not available to execute correction.

Subsection 5.2.a, added schedule interval for mission critical and Level II assessments.

Updated Section 7, References, to align with *Department of Commerce (DOC) Manual of Security, Policies and Procedures*, Chapter 7, "Occupant Emergency Plans and Procedures," Chapter 30, "Physical Security Policies;" Appendix K, "Department of Justice Standards for Protection of Federal Facilities," and Appendix S, "Occupant Emergency Plan Appendices."

Added Section 8, Office of Security/Regional office contact information.

Signed by John McNulty 10/14/08
John McNulty Date
Director, Office of Operational Systems

Facility Physical Security

Table of Contents: Page

1. Introduction. This instruction implements National Weather Service (NWS) Policy Directive (NWSPD) 30-51, *Physical Security*. It establishes a Physical Security Program for NWS field offices and provides guidance on operating procedures, reporting requirements, and responsibility assignments necessary to achieve an acceptable degree of security relative to the importance and value of field office resources.

2. Scope. This instruction provides guidance on facilities physical security, primarily for field offices. It establishes procedures for documenting field office incidents and reporting to responsible levels of authority having oversight for facility physical security.

3. Purpose. The intent of this instruction is to protect field office property, (e.g., real property, equipment, sensitive property) from break-in, attempted break-in, theft, or vandalism, and to protect Government personnel from physical threats or personal injury resulting from breaches in security.

4. Property: Includes Real Property (Buildings) and Personal Property (Equipment)

4.1 Building Security. The Department of Justice (DOJ) Vulnerability Assessment of Federal Facilities Report developed a security level rating system for federal facilities and established minimum security requirements for each level. Based on the DOJ Vulnerability Assessment Report, the Department of Commerce (DOC) established the security level rating

and minimum security standards for every DOC controlled facility. A level II designation is applied to most NWS field offices (e.g., Weather Forecast Offices, Tsunami Warning Center). Level II is a building that has 11 to 150 employees, a moderate volume of public contact, 2,500 to 80,000 square feet of space and activities that are routine in nature, similar to business activities. A Level 1 facility, a typical Weather Service Office, is defined as a facility with 10 or fewer Federal employees, 2,500 or less square feet of office space, and a low volume of public contact. Security requirements for each level are spelled out in *DOC Manual of Security, Policies and Procedures*, Appendix K, Department of Justice Standards for Protection of Federal Facilities.

4.2 Sensitive Property. Portable, self-contained items having high potential for theft or those that can easily be converted to private use are considered sensitive property and are subject to this policy. This includes cell phones, pagers, projectors, laptop computers, and personal digital assistants (PDA). All laptops, PDAs and smartphones need to have the current user assigned and recorded in the NOAA personal property recording system (Sunflower). Sensitive property does not include hand tools, assemblies, components or parts.

4.3 Physical Security Equipment. Physical security equipment is an important component of the implementation of this instruction. These systems include video/digital surveillance cameras and recording devices, physical security locks (keyed, cipher and electronic), and access card systems for buildings, real property, and gates.

5. General Instructions.

5.1 Field Offices and National Centers will:

a. Identify a focal point for physical security who will ensure field personnel are informed of physical security policy, instructions, local physical security operations, and lessons learned from past incidents.

b. Ensure compliance with *DOC Manual of Security Policies and Procedures* to include Occupant Emergency Plans, Procedures and Shelter-in-Place. Annual emergency evacuation drills should be executed and documented as well as actual real evacuations or Shelter-in-Place events.

c. Maintain an accurate inventory of physical security equipment with descriptions of current condition and operational readiness. Ensure all existing physical security systems are inspected and maintained properly. Document deficiencies in the Engineering Management Reporting System (EMRS) for proper incorporation in the Annual Work Plan (AWP) for the region.

d. Prepare an incident report using the (DOC/OSY) Regional Security Office form. If the office is located in a General Services Administration (GSA) controlled / managed building (where security is provided by GSA), use GSA Form 3155. Indicate any break in, attempted break in, or physical threat to government personnel or properties. Field offices and National Centers will forward the report via e-mail to the Regional or National Center HQs (as appropriate) and provide a copy to the supporting DOC Regional Security office. Complete the incident report including the

nature, time, and time line of actions taken after the incident. Also, include a list of property taken personal injury suffered, and other information pertinent to the incident. A copy should be maintained on-site.

e. Respond to the DOC Office of Security (OSY) surveys to identify and document physical security deficiencies and formulate recommendations to improve operations. Coordinate with and forward recommendations to the Regional or National Center HQs focal point (as appropriate).

5.2 Regional and National Center HQs will:

a. Identify a focal point for physical security to support the Regional Security Office in the performance of physical security assessment of field offices. The DOC/OSY team performs Anti-Terrorism Risk Assessments (ATRA) based on a criticality. Mission critical facilities are assessed annually while other Level II facilities are assessed once every three years. The DOC/OSY report will conclude with recommendations. Regional and National Center HQs will analyze the recommendations contained in the analytical risk assessment, develop a budget to implement the agreed to security measures necessary to improve field office physical security.

b. Maintain a record of incident reports filed by field offices. Analyze and recommend changes for improvement in physical security that will enhance mission readiness. Coordinate with the national focal point to respond to ATRA surveys and letters.

c. Prepare budgets to address deficiencies or planned upgrades to security systems noted above. Forward budget requests annually to NWS HQs. Use EMRS, if applicable, to document/record agreed to physical security enhancements. Incorporate the list in the AWP for the region, or classify the work as “deferred”, if funds are not available to execute.

5.3 Director, Office of Operational Systems will:

a. Assign the Chief, Facility Management Branch as the National focal point for the Facilities Physical Security program who will coordinate policy and instructions with DOC/OSY, Regional and National Center HQs.

b. Assess the impact of physical security deficiencies on mission readiness, prioritize budget actions to repair or replace security equipment, and support regional funding requests to implement corrective measures.

c. Maintain a national record of DOC/OSY inspections, findings, and costs. Respond to OSY reports by obtaining/coordinating response from Regional and National Center HQs.

6. Reporting. Field offices will use DOC/OSY Regional Security Office's on line reporting format to record incidents, if applicable. In GSA controlled / managed facilities (where security is provided by GSA), use GSA Form 3155; Offense / Incident Report.

7. References.

a. NWS Policy Directive 30-51, Physical Security, dated 8FEB08

b. NWSPD 1-1, Policy Formulation.

c. DOJ Vulnerability Assessment to Federal Facility Report.

d. DOC Security Handbook.

e DOC, Phased Facility Security Program Development Handbook.

f. Interagency Security Committee, Security Design Criteria for New Federal Office Buildings and Major Modernization Projects.

8. Department of Commerce Regional Security Offices.

Office of Security at NOAA
1335 East West Highway
Silver Spring, MD 20910
301-713-0954

Eastern Region Security Office
200 Gramby Street
Room 407
Norfolk, VA 23510
757-441-3420

Mountain Region Security Office
325 Broadway, Building # 1
Boulder, CO 80305
303-497-5198

Western Region Security Office
7600 Sand Point Way, NE
Building 1
Seattle, WA 98115
206-526-6571