UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
CHIEF ADMINISTRATIVE OFFICER

January 27, 2009

MEMORANDUM TO: NOAA Supervisors and Management Officials

SUBJECT: What to Do When a Laptop Is Identified as Missing

FROM: William F. Broglie
NOAA Chief Administrative Officer

The following guidance updates guidance originally issued in October 2006 concerning the appropriate steps to follow when a laptop computer, Personal Digital Assistant (PDA), or other hand-held information storage device is identified as missing, lost, or stolen. This guidance has been coordinated with Joseph Klimavicz, NOAA's CIO, to ensure consistency with current procedures. It is intended to support management officials in executing their responsibility in response to such incidents. You, as NOAA managers and supervisors, are responsible to ensure full compliance with these procedures.

STEP ONE: Initial Notification.

All lost, stolen, or missing laptops, PDAs, or other hand-held information storage devices must be reported to the NOAA Computer Incident Response Team (N-CIRT) via NOAA Form 47-43 (IT Security Incident Reporting Form) on the NOAA web page: https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html, immediately upon confirmation of status, e.g., Lost, Stolen, Missing). This requirement applies whether the device was issued to a NOAA employee or a NOAA contractor employee. The N-CIRT will provide you additional guidance, as needed in assessing the type of information on the device. (See Step Two below.)

If the identified device contains personally identifiable information (PII) the N-CIRT should be notified via telephone (301-713-9111) and leave an urgent page notification, if required. Following telephone notification to the N-CIRT, you must immediately complete the electronic NOAA Form 47-43 (IT Security Incident Reporting Form) on the NOAA web page: https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html.

STEP TWO: Initial Incident Assessment

There are four objectives of this step: (1) Confirm or identify whether the device contains Personally Identifiable Information (PII). PII is generally defined as information about an individual maintained by the agency that contains an individual's name **and** one of the following: social security number, date and place of birth, and mother's maiden name. Other information considered PII includes financial transactions, medical history, biometric records,

and criminal and detailed employment information that could be used to trace an individual's identity. (2) Identify whether the device contains other sensitive data (such as procurement-sensitive or pre-release budget data). The N-CIRT will assist with identifying the type of information on the device. (3) Identify the circumstances leading to the loss, specifically whether theft is suspected. (4) Identify any immediate mitigation steps warranted to prevent against recurrence of loss/theft.

STEP THREE: Notification of Security and Law Enforcement Officials

If theft is suspected, you should immediately contact the servicing security office (Office of Security (OSY), DOC) and local law enforcement officials; if directed by OSY, you should also contact the Federal Protective Service.

STEP FOUR: Appropriate Immediate Mitigation Action

Based on the initial incident assessment information, you should take immediate actions appropriate to mitigate against further loss/theft and/or to prevent exploitation of potentially compromised information, e.g., system passwords. This could include reviewing current security procedures to ensure compliance: e.g., securing/locking office doors, changing system passwords, etc.

STEP FIVE: Notification of Incident Involving Other Sensitive Data (but not PII)

Based on the nature of the other sensitive data contained on the device, you should notify, as soon as possible, appropriate NOAA officials. In the case of procurement sensitive data, you should notify the servicing Acquisitions and Grants Office location. In the case of pre-release budget data, you should notify your Line Office Chief Financial Officer, or NOAA Budget Officer. In the case of IT access credentials or other information related to accessing NOAA systems, you should notify your Line Office Information Technology Security Officer (ITSO) and the NOAA Computer Incident Response Team (N-CIRT)

STEP SIX: Conduct Follow-On Management Fact-Finding

Once appropriate officials have been notified of the loss/theft, and appropriate immediate actions have been taken to mitigate against further loss/theft, you must conduct additional fact-finding. The purpose of this fact-finding (management review) is as follows: (1) assess whether any additional preventive/mitigation measures should be taken, (2) assess the appropriate locus of liability for the loss of the device (for subsequent NOAA Board of Review action, as required under current DOC Personal Property procedures), and (3) assess whether any management action is warranted against specific individuals. Any questioning of employees as part of the management fact-finding process should be fully coordinated in advance with the servicing Workforce Management Office staff.

STEP SEVEN: Management Documentation Requirements

CD-52. Management officials must complete a CD-52 (Report of Review of Property) following completion of the management review to document (1) the circumstances surrounding the

loss/theft of the device, (2) the steps taken to recover the device, (3) the assessment of personal liability and negligence on the part of specific individuals (federal employees, contractor employees). The completed CD-52 must be submitted to the NOAA Property Management Office within 10 business days of the incident. Form CD-52 can be found at http://www.pps.noaa.gov/New_menu/cd52fll.pdf .

Confidential Memorandum to CAO. Management officials must also complete a confidential memorandum from the Assistant Administrator (or DAA)/ Staff Office Director documenting the actions planned by management officials to (1) correct causal/contributing factors to the loss/theft; and (2) administrative actions (counseling letter, etc.) planned regarding federal/contractor employees. This memorandum is to be submitted to the NOAA Chief Administrative Officer (CAO) within 15 business days of the incident.

STEP EIGHT: NOAA Board of Review

The NOAA CAO shall cause to be convened a Board of Review to determine individual negligence (simple or gross) and extent of personal liability for the loss/theft of the device. The Board shall be convened monthly, or as needed, and be composed of a senior management representative from each Line Office, CIO, CFO, OGC, and CAO. The Board shall examine all facts (and determine the need for additional information), determine the level of negligence, and recommend the level of liability for the cost of replacement of the lost/stolen device. The Board shall forward its recommendations to the CAO for final decision and implementation.

If you have questions, there are individuals who can assist you. While any of the individuals should be able to assist you, we have identified particular areas of expertise:

- N-CIRT, 301-713-9111 (IT security incidents, assistance in identifying PII and other types of data/information on devices);
- Glenda Patrick, Deputy Director, Logistics Division, and NOAA Property Management Officer, 301-713-3551, x171 (personal property matters, including fact finding);
- David W. Johnson, 757-441-3870 (employee relations matters);
- Larry Reed, Director IT Security, 301-713-0042 (general IT security matters).

Please do not hesitate to call these individuals in the event of a lost/stolen laptop or other hand-held device, or for general questions regarding the incident response procedures.