Department of Homeland Security
Management Directives System
MD Number: 11010.1
Issue Date: 03/25/2003

ISSUANCE AND CONTROL OF CREDENTIALS

I. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the issuance and control of credentials.

II. Scope

This directive applies to all DHS Headquarters elements and to any organizational elements that do not have existing procedures and requirements regarding the issuance and control of credentials. Any organizational element that has existing credentialing procedures and requirements may continue them in force until the DHS Office of Security issues permanent, Department-wide policy in this area.

III. Authorities

The Homeland Security Act of 2002, codified in Title 6, U.S. Code

IV. Definitions

Credential: Identification showing that an individual is entitled to represent, or exercise official power as, part of a United States Government agency.

V. Responsibilities

A. ***The Secretary*** (or his/her designee) will designate a DHS Office of Security. This office will coordinate the design and issuance of credentials.

B. ***The Under Secretary for Management***, through the DHS Office of Security, is responsible for all aspects of this directive.

VI. Policy & Procedures

A. ***Procedures***:

1. Issuance of Credentials. As soon as practicable, the DHS Office of Security will issue to each employee an identification which contains the photograph, name, and signature of the employee. Additionally, law enforcement personnel are required to have badges and commission books.

Access control officials will be advised of pending new appointments by copies of appointment letters forwarded by the Office of the Under Secretary for Management. On the first day of duty, new employees will be processed to obtain the necessary photographs and signatures that will be made a part of the credentials.

2. Control of Credentials. All credentials are considered to be accountable property. Because of operational security concerns and the grave potential for misuse if lost or stolen, all credentials are to be treated with the same level of care that an employee would assign to a firearm or other dangerous weapon. Inappropriate use or misuse of credentials, in particular the sale or transfer of credentials to unauthorized persons, shall result in employee discipline, to include removal.

In the event of loss, theft, or destruction of credentials:

a. The employee responsible for the credential, or the employee discovering the condition, will:

(1) (Notify (as soon as practicable, but within no more than 24 hours) the appropriate property management officer and the supervisor of the office in which the incident occurred. (Care should be taken to ensure that those supervisors in the employee's chain of command see all notification documents).

(2) Take immediate action to affect recovery of the lost or stolen credential, and obtain all available information concerning the credential's loss, theft, or damage for inclusion in required reports.

b. The employee's supervisor will:

(1) Notify the DHS Office of Security immediately.

(2) Ensure that an official message is submitted to the DHS Office of Security. The message must include the approximate time and date the credential was discovered missing and the location where the credential was last seen.

(3) If applicable, advise the DHS Office of Security to transmit a description of the credential to the National Crime Information Center (NCIC). (Applicability is based upon the circumstances of the incident; NCIC entry must take place within 24 hours of the supervisor's notification.)

3. If applicable, the property management officer will ensure that local law enforcement is notified of a lost or stolen credential. (Applicability is based upon the circumstances of the incident.)

4. The DHS Office of Security will ensure that the above requirements have been met prior to authorizing issuance of a new credential.

B. ***Questions or Concerns Regarding the Process***. Any questions or concerns regarding this directive should be addressed to the DHS Office of Security.