ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

Distribution:
All Department of Education Employees

Signed by: Denise L. Carter
Principal Deputy Assistant Secretary for Management
Delegated the Authority to Perform the Functions and Duties of the Assistant Secretary for Management

Identification Media (Credentialing)

Table of Contents

For technical information regarding this ACS document, please contact the Physical Security Officer on 202-401-3611 or via email.

Supersedes OM: 3-103 “Identification Media (Credentialing)” dated 03/18/2009.

I. Purpose

This Directive sets forth the policy and organizational responsibilities for the issuance of the U.S. Department of Education's (ED) Identification (ID) Media Credentialing, the US Government "Personal Identification Verification" (PIV) Identification Card, and the process for individuals visiting ED facilities in compliance with the Federal Management Regulation, Subchapter C- Real Property, Part 102-74—Facility Management.

II. Policy

It is the policy of ED to issue Identity (ID) Media, which includes any Shield, Credential, or ID card, including Homeland Security Presidential Directive 12 (HSPD-12) Personal Identification Verification (PIV) cards, to employees (Federal and Contract) located in headquarters and in the regional, field, and area offices. Visitors at ED will receive either an "Escort Required" or "No Escort Required" badge, as applicable.

All ID cards must be displayed in clear view while in ED-occupied facilities in headquarters and in the regional, field, and area offices. Federal government employees of other agencies must either show Federal Law Enforcement credentials or visibly display their government ID card and the "No Escort Required" badge issued by ED.

III. Authorization

This Directive is authorized by Executive Order 12977 (October 19, 1995) establishing the Interagency Security Committee (ISC) to develop and oversee the implementation of security standards for Federal facilities; Title 40 U.S.C. Sections 19, 285, 486 and 490; 41 CFR 101-20.302; Homeland Security Presidential Directive-12 (HSPD-12 issued December 2004), Department of Justice Vulnerability Assessment of Federal Facilities Report at table 2-8 (June 28, 1995) (http://www.usdoj.gov/opa/pr/Pre_96/July95/381.txt.html), and Departmental Handbook for Property Management.

IV. Applicability

This Directive applies to all employees, contractors, retirees, and others who are authorized access to ED-occupied facilities in headquarters, regional, field, and area offices.

V. Definitions

A. **Badge or Card:** For the purposes of this Directive, an ID badge and an ID card are the same. A badge (not a law enforcement shield or credential) is generally displayed vertically and a card is generally displayed horizontally.

B. **Credentials (Enforcement):** Shows proof of authority and is issued only to Special Agents, Inspection Personnel, Deputized U.S. Marshals, Police, and Criminal Investigation personnel in the GS-1801, GS-1811, GS-1802, GS-0080 Federal job series.

C. **HID:** Is both a company name and a process named after the company (HID is not an abbreviation), which utilizes radio frequency identification (RFID) technology for physical access control. Proximity and ***iCLASS*** technologies can be housed on the same credential and combined with other technologies such as a magnetic strip, a barcode, or contact smart chip modules.

D. **ED Access Card:** Designed for entry control into all ED access controlled facilities and issued to persons not meeting PIV requirements, authorized temporary employees, and authorized contractors.

E. **ID Media:** Includes any card/pass, shield, credential, ID card or similar items, which contain the ED name, seal or symbol; may be used to identify the bearer; and is normally carried or worn by the bearer. ID Media may also contain one or more of the following: the bearer's photo, name, card serial number, an authorizing or validating signature, and information to indicate the purpose of the badge. The Public-Key Infrastructure (PKI) certificate, personal fingerprints, and Social Security Number (SSN) will be encrypted internally to the media and not visible to public display.

F. **Shield (Enforcement):** Provides an outward, visible sign of authority and is issued at ED to inspection, criminal investigation personnel and authorized security personnel in the GS-0080, GS-1801, GS-1802, GS-1811 Federal job series, and OIG personnel designated by the Inspector General.

VI. Responsibilities

A. **The Assistant Secretary for Management** is authorized to prescribe ID Media for use within ED, to include Credentials (Non-Enforcement) and Shields for use within Office of Management/Security Services.

B. **The Inspector General** is authorized to prescribe and issue the OIG Credentials and shields for OIG personnel designated by the Inspector General.

C. **The Secretary's Protective Detail,** Office of the Secretary (OS), is authorized to prescribe Credentials (Enforcement) and Shields (Enforcement) for protective detail personnel.

D. **Office of Management/Security Services (OM/SS)** is responsible for:

1. Planning, developing, implementing, evaluating, and controlling the ED-wide ID Media Program and the US Government PIV ID Card;

2. Ensuring that individuals meet personnel security requirements before authorizing the issuance of ED ID cards and meet the HSPD-12 requirements for issuing the US Government PIV ID Card;

3. Installing, maintaining, and managing all ID Media equipment systems;

4. Ensuring integrity of the data in the system; and

5. Issuing ID Media while ensuring that ED ID cards are issued only upon review of personnel security files and in coordination with the OM/SS Director, Personnel Security and Emergency Preparedness.

E. **The Principal Office (PO) Executive Officer/Administrative Officers** are responsible for:

1. Ensuring that personnel within their PO possess only authorized ED ID media; and

2. Returning ID Media to OM/SS when employees and contractors (*in coordination with the COR*) leave ED or are terminated from service.

F. **Managers** are responsible for ensuring that employees use the ID Media and display it properly. Each manager is responsible for reporting unauthorized use of ID Media to OM/SS and if located in a regional office, the Regional Security Coordinator and OM/SS.

G. **Employees** are responsible for reporting immediately/as soon as practicable, to both OM/SS and the Executive Officer/Administrative Officer, lost, stolen, or destroyed ID Cards or Credentials. Employees are also required to notify the Regional Security Coordinator, of lost, stolen, or destroyed ID Cards or Credentials when applicable.

VII. Procedures and Requirements

ED ID Media is issued solely for use by individuals in the performance of official duties that do not meet the requirements in HSPD-12 for the US Government PIV ID Card and for personal ID. ID Media may not be used for retirement

mementos, honorary presentations, or similar purposes. The ID material issued by ED is the sole property of the US Government.

The ID database may not be used for administrative purposes with the exception of an official law enforcement investigation or ED OIG audit, inspection, investigation, or management activity, in which a formal request for the specific data must be transmitted to OM/SS PKI certificates will be used by OCIO for system access.

A. **Restrictions**

1. No employee may have in his/her possession more than one Department of Education issued ID card or ED issued PIV ID Card, and not more than one set of ED official Credentials. This Directive does not restrict ED employees from having building access cards issued by building management in private and GSA leased facilities.

2. ED employees may not display any form of ID associating them with ED, which has not been officially authorized by the Assistant Secretary for Management or the Inspector General. Development of new ID Media or methods of use, assembly or display, or modifications of existing media or methods of use or display must be submitted through the Executive/Administrative Officer of the requesting organization to OM/SS for coordination and approval.

3. The Assistant Secretary for Management is the approving authority for the printing or reproduction of any type of ED ID media or US Government PIV ID Card (with the exception of OIG issued credentials and shields). Requests to print or reproduce must be ***submitted in writing*** to the Assistant Secretary for Management for approval.

B. **Penalties**

1. 18 U.S. Code, Section 499, prescribes a fine or up to five years imprisonment, or both, for whoever falsely makes, forges, counterfeits, alters, or tampers with any naval, military or official pass or permit, issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates, or falsely represents himself to be or not to be a person to whom such pass or permit has been duly issued; or who willfully allows any other person to have or use any such pass or permit issued for his use alone.

2. 18 U.S. Code, Section 701, prescribes a fine or up to six months imprisonment, or both, for whoever manufactures, sells or possesses any badge, ID card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any

officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, ID card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law.

C. **Protection of ID Media**

Any individual who recovers any type of ID Media must report it immediately to OM/SS, so that local accountability records are adjusted to reflect the recovery. Regional employees must contact their Regional Security Coordinator, OM/SS by Email to EDIDOffice@Ed.gov or Security.services@ed.gov or via telephone at (202) 401-3610 and follow the protocol established within their respective facilities (i.e. GSA regulations, or private leased facilities).

OM/SS will destroy the recovered media (except Shields, which may be placed back in stock and reissued). The OIG will destroy all OIG recovered credentials and media except for Identification/Access Cards which will be returned to OM/SS.

In all cases of lost or stolen ID Media, the Executive Officer/Administrative Officer, /Regional Security Coordinator, must notify the OM/SS immediately/as soon as practicable with a written memorandum or email request to deactivate the ID Media.

1. Employees must take precautions to prevent loss, theft and destruction of Credentials, ID cards, Shields (Enforcement), and other types of ID Media. In the hands of an unauthorized person, these items have the potential of bringing serious discredit and adverse publicity to ED. ID Media must either be in the possession of the authorized employee or safeguarded to insure no unauthorized use may occur. ID Media must ***never*** be left unattended in briefcases, unlocked desk drawers, automobiles, etc.

2. If an employee's ID card or Credentials is lost, stolen or destroyed, **the employee must report this immediately (no later than 2 business days or as soon as possible**) to the supervisor, principal office executive officer and/or OM/SS, explaining the circumstances and recovery attempts. If an employee's Shield (Enforcement) is lost, stolen or destroyed, the employee will report this immediately upon entry to an ED facility in writing through supervisory channels to OM/SS. The initial report can be done via email to ED ID Office for internal ED users or via email outside of ED at EDIDOffice@Ed.gov.

In the case of a lost or stolen ID card with restricted access authorized, the employee's manager will notify the manager of the restricted area as identified on the ID application form.

The employee's Executive Officer/Administrative Officer must also be notified by the employee no later than 2 business days or as soon as possible to arrange for replacement of lost a ID card if necessary. The employee must fill out a new ID application form as shown in Appendix A, marking "replacement ID" and attach a statement explaining the circumstances and recovery attempts.

3. Managers must counsel employees concerning safeguards when there is a repeated loss of ID cards, Credentials, Shields (Enforcement and Non-Enforcement), or other ID Media.

4. For Office of Inspector General (OIG) Criminal Investigators and applicable staff that carry Federal Credentials, The OIG will ensure that (1) any lost or stolen credentials and/or shield is promptly reported to the employee's immediate supervisor and OIG's Management Services is promptly notified; and (2) the lost or stolen credentials and/or shield is entered into the National Crime Information Center (NCIC) and that NCIC records are properly annotated. Should a lost or stolen Credential and/or Shield be recovered OIG will also be responsible for making sure the NCIC record is properly annotated to record the recovery.

5. Mailing ID Media stock, Credentials and/or Shields, requires a controlled means. Blank ID Media stock, Credentials and Shields will be in double-sealed envelopes and sent via registered mail. ID cards sent between offices must be sent with a transmittal form and must be in double-sealed envelopes.

D. **Supplies**

OM/SS will supply ID Media, media holders and lanyards to Regional and Area Offices on an as needed basis.

E. **Records and Accountability**

1. The accuracy of ID card records, Credentials and Shield (Enforcement) records will be audited annually by the ID "Systems Owner Representative" (OM/SS), and reconciled at the end of the fiscal year against the numerical and alphabetical files and ID database as outlined below. All records of such audits will be handled as Sensitive But Unclassified (SBU) and will be kept for three years in an approved container.

Every employee will be issued either an ED ID card or US Government PIV ID Card (***issuance of PIV ID cards is mandatory under Federal regulations – HSPD-12- for all contractors and employees that are covered by the Directive***), after completion of the ID card application and review and adjudication of the minimum background investigation, the employee will be issued a PIV ID card. The ID card application form, Parts (1) (2) and Form B (if applicable), will be the primary records inventoried.

For OIG employees, OIG will maintain a record of all OIG Credentials (Enforcement) and Shields (Enforcement). This will also satisfy requirements for accountability of the Credentials.

OS will maintain a record of all security detail Credentials (Enforcement) and Shields (Enforcement) for the Secretary's Protective Detail. This will also satisfy requirements for accountability of the Credentials.

All Contracting Office Representatives (CORs) will develop and re-validate their list of contract employees every six months and immediately notify OM/SS when a contract employee has been removed, added, and/or is no longer authorized access. If contractor lists are not properly validated and verified through OM/SS, contractor access will be denied until verification has been assured. It is the responsibility of the COR, to ensure the contractor photo ID card is recovered and returned to the Executive/Administrative Officer for submission to OM/SS within 24 hours of when an employee is no longer authorized access.

Upon request, OM/SS will provide a report to the Executive/ Administrative Officer listing the authorized access level for individuals.

2. The "ED ID Card Application form" (in conjunction with the proper Personnel Security clearance forms) will be used when issuing ID Media. The employee, the employee's Executive Officer Administrative Officer, OM/SS (or designated official), and the restricted area manager, where applicable, will all sign the ED ID Card Application forms.

   The blank ED ID Card Application Form is available for use by ED personnel on ED intranet site (connectED, Forms) and can be printed and manually completed.

F. **ID Cards**

1. Overview

ID cards will be issued to all ED employees and authorized contractors. Badges will be worn on the outer garment, in clear view at all times, while in ED facilities in headquarters and in the regional, field, and area offices.

To maintain the integrity, respect and acceptance of the ID card, much effort will have to be expended to make certain that unauthorized personnel never have access to the card stock and equipment and that an employee, never has more than one ID card in his/her possession. The employee's manager must recover the employee's ID card and/or credential when he/she leaves ED.

2. Responsibilities

   a. The Executive Officers and Administrative Officers have responsibility for collecting ID cards of intermittent employees, employees who resign or retire, or employees placed in non-work status (i.e., seasonal, LWOP, suspensions of 30 calendar days or more or non-work status) as well as employees on their last workday. The Executive Officer/Administrative Officer is responsible for sending the recovered ID cards to OM/SS for disposal within 2 business days of collection.

   b. All managers and CORs have responsibility for the following:

      (1) Ensuring that contract company employee under their management are issued ID cards and wear their ID cards properly at all times.

      (2) Assuring ID cards of contractors who resign or retire, or contractors placed in non-work status (i.e. seasonal, LWOP, suspension, 30 or more days of extended leave), as well as contractors on their last workday, are turned into the Executive Officer for that PO. This is in concert with the Contract Company security officer and/or liaison.

      (3) Determining that only authorized personnel are in the work area for which they are responsible, and immediately asking suspected unauthorized persons in their area for a proper ID.

      (4) Informing all employees under their control of the importance of good security practices.

   c. All employees and other persons issued ID cards are responsible for:

      (1) Safeguarding their ID cards.

(2) Wearing their ID cards properly at all times, within ED facilities in headquarters and in the regional, field, and area offices.

(3) Promptly (no later than 2 business days or as soon as possible) reporting loss of their ID cards to their supervisor and OM/SS.

(4) Immediately reporting to their supervisor the presence of unauthorized personnel in the work area.

(5) Return their ID cards to their Executive Officer/Administrative Officer when placed in a non-work status. Regional employees will return their ID cards to their Regional Security Coordinator or the Executive Officer/Administrative Officer if present, who will return ID Cards to OM/SS upon termination of employment.

d. If an employee with a photo ID card is detailed or traveling to another facility, he/she can make arrangements through OM/SS (regional employees will work through their Regional Security Coordinator) to have temporary access granted to their ID card for the off-site facility, provided that proper procedures for restricted access areas are followed and approval is granted by the restricted access manager for the area.

3. Wearing of ID

a. All persons will wear ED issued ID cards when in ED facilities or spaces in headquarters and in the regional, field, and area offices. ID cards will be worn fastened to either a belt, item of clothing or chain/lanyard worn around the neck.

b. ID cards must be worn on the outer garment, in clear view, in such a manner that the photo is clearly visible from the front at all times, and is available for inspection by security officers while in ED spaces in headquarters and in the regional, field, and area offices. No mementos or other items may be attached to the ID card that would obscure the information on the card.

c. The employee's supervisor, Executive Officer/Administrative Officer, and OM/SS must approve exceptions to these requirements for reasons of health, safety, or religion.

4. Descriptions and Use of ED ID Cards and US Government PIV ID Cards

a. The ED ID card is authorized for the following uses:

(1) Visual ID for entry control into all ED facilities and offices in headquarters and in the regional, field, and area offices;

(2) Entry control in ED facilities, in headquarters and in the regional, field, and area offices, including all restricted areas;

(3) Visual ID of authorized bearer within the work area; and

(4) Automated HID proximity compliant electronic access control into all access controlled ED facilities, spaces, and restricted spaces; and

b The US Government PIV card is authorized for the following uses:

(1) Visual ID for entry control into Government owned and leased facilities, all ED facilities and offices in headquarters, regional, field, and area offices.

(2) Entry control in ED facilities, in headquarters and in the regional, field, and area offices, including all restricted areas.

(3) Visual ID of authorized bearer within the Federal Government and ED work area.

(4) Automated HID proximity compliant electronic access control into all access controlled ED facilities, spaces, and restricted spaces, personal identification in Government facilities.

(5) Personal ID for use in conjunction with official duties.

c. All Government employees and contractors who qualify for a US Government PIV ID Card will be issued a US Government PIV ID Card.

(1) Employees will be issued a white photo ID card with a blue photo background and a white name block background clearly identifying the individual as an ED employee.

(2) Non-Federal personnel (such as a contractor) who are authorized a US Government PIV ID Card to access ED facilities will be issued, as authorized, a white photo ID card with a blue photo background and green name block clearly identifying the individual as a contractor.

(3) Foreign Service Nationals (such as cleared non-citizens) who are authorized a US Government PIV ID Card to access ED facilities will be issued, as authorized, a white photo ID card

with a blue photo background and blue name block clearly identifying the individual as a Foreign Service National.

(4) Special purpose US Government PIV ID Cards such as Emergency Responders will have red vertical stripe on the bottom of the card indicating emergency responder.

d. All term employees and contractors that do not meet the HSPD-12 term requirements will be issued an ED ID card.

(1) The term employee will be issued a white photo ID card, clearly marked on front and back, to identify the individual as an ED employee; a blue photo border indicates general access.

(2) Other Federal employees assigned to ED that do not qualify for a US Government PIV ID card (such as interns, or detailed Federal employees who do not have a US Government PIV ID Card) will be issued white photo ID cards with a green photo border, for general access. These ID cards do not identify the individual as an ED employee.

(3) Non-Federal personnel (such as a contractor) who are authorized to access ED facilities will be issued, as authorized, a white photo ID card with a red photo border.

(4) Solid red or grey non-photo ID cards, including those issued to guards, are for access control only and may not be removed from the facility.

e. The ED ID card and US Government PIV ID card are the same size and has the same appearance as a standard plastic credit card. It has an HID identified serial number and is embedded with a programmable memory with magnetic field affixed to the inside which allows encoding that permits the card to be used as a key card to open doors, or for other control purposes. The US Government PIV ID card has the same features as the ED ID card and contains an imbedded microchip to store PKI certificates and PIV information. The back of the ID card has the HID/serial and agency specific issuing number etched and is printed with a return address, warning for misuse, and privacy act information.

f. The front of the Employee ID card has a color photo of the individual to whom it is issued, and the individual's ***typed*** legal name. The data area, on the face of both the ED employee ID card and US Government PIV ID card, has an ED seal. The ED ID card has a blue photo border and a blue highlight with the word,

EMPLOYEE imprinted in white across the bottom of the card. The US Government PIV ID card has a color photo and a blue background and border around the picture both are used for general and restricted access cards. The upper 60 percent of the ID card is the photo area, ED ID area, and ED seal. The lower 40 percent is the data area, which could also include the letters "LE" on the ED ID and Emergency Responder on the US Government ID. Note: The letters "LE" indicate that the bearer is an authorized Law Enforcement employee and does not have to pass through personnel screening.

g. The front of the Contractor ED ID card is identical to the employee ID card, with the exception of the color, which is white with a red photograph border, and may not contain the "LE" status. The US Government Contractor PIV ID Card has a green background behind the name block.

h. The front of the "Temporary employee" ED ID card is identical to the "Employee" ED ID card, with the exception of the color, which is white with a green photograph border, and could contain the "LE" status.

i. Personnel hired directly by ED under programs such as Stay-in-School, Federal Summer Intern Program, temporary appointments of 90 days or less, intermittent, or students appointed under the Co-Operative Work Study Program, or similar programs are considered ED employees and at OM/SS' option, may be issued the employee ED ID card. Persons that are Government Employees for a period of less than one year will not be issued a US Government PIV ID card.

5. "Visitor Escort Required" and "Visitor No-Escort Required" ID Badges

a. All visitors who are not Federal government employees will be issued a "Visitor Escort Required" badge (or the GSA equivalent).

b. All visitors who are Federal government employees must present their own agency ID and will be issued an "Escort Required" badge (or the GSA equivalent) unless prior arrangements have been made with OM/SS.

c. Employees who forget or lose their ID card assigned to an ED facility or ED restricted area in headquarters and in the regional, field, and area offices will be issued a one-day access badge upon verification of employment by a coworker or the visitor services staff.

d. "Temporary" (daily replacement for lost or forgotten ED or PIV ID issued no more than twice within two consecutive days) and "Visitor and Escort Only ID" badges ***may not be removed*** from the issuing facility. They must be returned when the individual departs the facility or restricted area.

e. Where regional offices issue temporary, "Visitor Escort Required" and "Visitor No Escort Required" ID badges, the above procedures will be followed.

6. ID Issuance Procedures

a. Obtaining a photo ID card

(1) Employee ED ID

(a) Must be a full or part-time government employee with ED.

(b) Must have completed appropriate background investigation forms for their position within fourteen days of entrance to duty in accordance with 5 CFR Part 736, Personnel Investigations, and OM/SS Personnel Security requirements. Employees not completing the required paperwork within fourteen days will have his/her EDNET and building access revoked.

(c) All applicants must complete the ID application form, and submit through the employee's Executive/Administrative Officer, to OM/SS.

(d) Employees requiring access to controlled spaces must complete the optional Form B and submit it to the appropriate controlled space manager for signature, prior to submitting it to the Executive/Administrative Officer and OM/SS for processing.

(2) Contractor ID

(a) Must be contracted directly to ED and work a minimum of three days per week, have a work space, computer, telephone and ED Email address assigned to them within one of ED's facilities. Contractors that do not fit the description above or are telecommuting for ED do not qualify for an ED ID and will be issued either an "Escort Required" or a "No Escort Required" badge when access

is needed provided the proper security paperwork is submitted to OM/SS.

(b) Must have completed appropriate background investigation forms for their position, within the time frame stipulated by the supplement to OM: 5-101, Contractor Employee Personnel Security Screenings. Contractors not completing the required paperwork within the required time frame will have his/her EDNET and building access revoked.

(c) Must complete the ID card application form and submit to the contractor's COR. The COR will submit the form to his/her Executive Officer/Administrative Officer for submission to OM/SS.

(d) Contractors requiring access during building secure hours, Monday through Friday after 8:00 p.m., and/or weekend or holiday access must complete Section B (Access Required).

(e) Bearers requiring access to controlled spaces must complete the optional Form B and submit it to the appropriate controlled space manager and their Executive/Administrative Officer for signature prior to submitting it to OM/SS for processing.

(f) All Contractor IDs will have an internal expiration date of one year and will require an Email notification from the COR to the ED ID Office stating that ED still maintains the services of the contractor. If a request for extension has not been received from the COR, the contractor's EDNET and building access will be revoked.

b. Processing Application and Issuing ID

Once all paperwork is completed and signatures from the Executive Officer/Administrative Officer, controlled space manager, and OM/SS are verified, the bearer will be notified to report to the ED ID Office located in LBJ, Room 1E102 to obtain his/her ID photograph. Regional employees will follow the protocol established within their respective facilities (i.e., GSA regulations, or private leased facilities).

A light colored backdrop (white) is used for all ED ID card photos while a light blue backdrop is used for the PIV ID card.

The type of card to be issued to ED employees, other Federal employees and to non-Federal personnel is specified in Section VII. F. 4. of this Directive, and no exceptions can be made without advance approval from the Assistant Secretary for Management.

(1) The photograph will be from the shoulders up and focus on the bearer's face.

(2) The purpose of the photo is to provide an immediate visual verification of the bearer's identity. Wearing of hats, scarves, caps, sunglasses, etc., obscure the face of the individual and minimize the effectiveness of the photo ID. These items may not be worn except for reasons of religion or health and must first be approved by the employee's supervisor, Executive Officer/Administrative Officer, and OM/SS.

(3) A mirror will be provided, and it is the responsibility of the employee for his/her grooming, and appearance. Due to the cost of the ID Media, once the photo is taken and the ID card is printed, no second photo or printing will take place, with the exception of improper picture format, unrecognizable photograph, bad ID Media parameters or misprint of the ID card, all of which will be at the discretion of the issuing official.

c. Visitor ID Badges

(1) Individual Visitors for Washington, DC Headquarters' ED Office located in LBJ Federal Building.

Visitors should be scheduled by the appropriate office or individual by contacting OM/SS, by Email to "Visitor Request VisitorRequest@ed.gov" with a cc to Christopher.Strambler@ed.gov and Kevin.Williamson@ed.gov with the following information: Name of visitor, time of arrival, entrance visitor will arrive at, and contact number of employee being visited.

(2) Individual and Group Visitors for all other Non-LBJ buildings (Regional Offices and other Headquarters' Offices located in Washington, DC)

Employees should follow the protocol established within their respective facilities (i.e., GSA regulations, or private leased facilities). Unscheduled visitors will be handled on a case-by-case basis

(3) Group Visitors for Headquarters' Facilities (Washington, DC area offices)

Sponsors of group visits must schedule entrance into ED spaces in advance, consistent with the Group Visitor Notification table below:

The sponsor must contact OM/SS, by email at ("Visitor Request VisitorRequest@ed.gov with a cc to Christopher.Strambler@ed.gov and Kevin.Williamson@ed.gov ") with the following information: Name of visitor(s), time of arrival, entrance visitor will arrive at, and contact number of employee being visited.

Group Visitor Notification Table	
Number of Visitors in Group	**Minimum Time to Notify Security**
20 or less	Two days prior
21 to 50	Three days prior
51 or more	Five days prior

Group visitors will be issued IDs and admitted by one of the following means:

(a) Sponsor will make group or conference badges and submit them to OM/SS (regional employees will submit through their Regional Security Coordinator) along with the proper list. Sponsor-made badges must contain the following information: location of meetings or conference (room number, auditorium), visitor name, date of visit, and title of conference, if applicable.

(b) OM/SS will make and print visitor nametags as the visitors arrive in conjunction with verification of the sponsor provided visitor request list.

(c) Visitors will be issued either an "Escort Required" or "No Escort Required" digitally printed stick-on badge or a pre-printed temporary visitor pass.

Visitors who are issued “Escort Required” badges must be escorted at all times by an ED employee, authorized ED contractor or authorized GSA employee.

Escort Duties and responsibilities:

i. Escorts must sign for entrance and accept full responsibility for their respective visitors.

ii. Visitors must be escorted at all times in controlled spaces.

iii. The escort must keep the visitor in view at all times, with the exception of the restrooms, in which the escort will accompany the visitor to the door and resume the escort responsibility upon the visitor’s exit from the restroom.

iv. The escort must accompany the visitor on exit from the facility to the same Visitor Services desk that processed the issuance of the visitor badge.

Group visitors for Regional and Field Offices

Regional employees should follow the protocol established within their respective facilities (i.e. GSA regulations, or private leased facilities).

d. Forgotten cards

(1) Headquarters employees reporting to work in LBJ without their ID card will proceed through full security screening then report to the Visitor Services desk at either the “C” Street or Maryland Avenue entrance to be issued a “No Escort Required ID” badge. Headquarters’ employees reporting to work in regional facilities or buildings other than LBJ, who do not have their ID card will contact OM/SS by E-mail at EDIDOffice@ed.gov or Security.services@ed.gov and telephone at (202) 260-5267 for verification of employee status. Employees must also follow the protocol established within their respective facilities (i.e., GSA regulations, or private leased facilities).

(2) Contract personnel visiting a facility and not on an access list will be issued an “Escort Required” ID badge. These individuals must sign the visitor's register, present a valid government-issued picture ID (such as a driver's license) to

verify identity, and must be escorted by an ED employee at all times. An ED employee assigned to the facility must corroborate the individual's need to access the site.

e. Damaged or inoperable cards.

ID Media that is malfunctioning or inoperable due to normal wear will be replaced without fee by presenting the ID card at the ED ID Office, LBJ Room 1E102, during normal working hours (or for regional employees, through their Regional Security Coordinator). If it is an emergency during Monday through Friday after 8:00 p.m., and/or weekend or holiday access hours, and access to controlled spaces is required immediately, the employee must contact the Executive Officer/Administrative Officer for further instructions. The new ID number must be recorded on the individual’s ID application when a replacement ID card is issued.

PRIVACY ACT INFORMATION

For contractors and non-government approved organizations:

The Privacy Act, *5* U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting Social Security Numbers (SSN's) is Executive Order 9397. In addition, the authority to collect each individual's "personally identifying information" is authorized under Executive Order 10450, section 2 and 3, Executive Order 12958, and Executive Order 12968, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended (42 U.S.C. § 5149(b) and the Privacy Act system of records, the Personnel Security System. The social security numbers and all "personally identifying information" will be used to identify individuals as required for the purpose of hiring and employment, including background checks. Such "personally identifying" information is required before each individual can be hired and granted access to agency-controlled facilities, computers, databases, and other agency systems. Although disclosure of social security numbers is not mandatory, failure to do so may impede the processing of each individual's application for employment. In addition, failure to provide complete "personally identifying" information may impede the processing of each individual's application for employment.

I have read and acknowledge the above Privacy Act statement and approve that my information be used to conduct a National Crime Information Center check prior to my access to ED facilities. I also agree to provide my fingerprints for the FBI Criminal History check and receive a favorable adjudication of the fingerprint results for continued access to ED facilities.

_____ _____

SIGNATURE DATE

For ED and Other government agency employees:

The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting Social Security Numbers (SSN's) is Executive Order 9397. In addition, the authority to collect each individual's "personally identifying information" is authorized under Executive Order 10450, section 2 and 3, Executive Order 12958, and Executive Order 12968, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, *as* amended (42 U.S.C. § 5149(b)). The social security numbers and all "personally identifying information" will be used to identify individuals as required for the purpose of hiring and employment, including background checks. Such "personally identifying" information is required before each individual can be hired and granted access to agency-controlled facilities, computers, databases, and other agency systems. Although disclosure of social security numbers is not mandatory, failure to do so may impede the processing of each individual's application for employment. In addition, failure to provide complete "personally identifying" information may impede the processing of each individual's application for employment.

I have read and acknowledge the above Privacy Act statement and approve that my information be used to conduct a National Crime Information Center check prior to my access to ED facilities. I also agree to provide my fingerprints for the FBI Criminal History check and receive a favorable adjudication of the fingerprint results for continued access to ED facilities. Should I already be employed, an unfavorable adjudication may result in my immediate release and termination from ED employment with no further appeal.

_____ _____

SIGNATURE DATE

Memorandum of Agreement

MEMORANDUM OF AGREEMENT

This agreement is between the American Federation of Government Employees, AFL-CIO, National Council of Department of Education Locals ("Union"), and the United States Department of Education ("Employer"), collectively described as "the Parties." It records the Parties' agreement with respect to the implementation of Homeland Security Presidential Directive 12 (HSPD-12) as it applies to Personal Identification Verification (PIV) cards. This agreement applies only to bargaining unit employees and positions.

1. Subject to the Employer's rights under Section 7106 of the Federal Service Labor-Management Statute, the Parties agree that:

   a. PIV cards will be used only for identification purposes and as a medium for obtaining access to buildings, facilities, and secured spaces;
   b. PIV cards will not be used for timekeeping;
   c. Data collected from the use of PIV cards will not be used for administrative purposes other than those permitted in by the agency's Identification Media (Credentialing) directive; and
   d. The Employer will not add additional personal data about cardholders to PIV cards beyond that mandated by Government-wide standards

   unless and until the Employer first notifies and negotiates, upon request, with the union to the extent required by law and the Parties' Collective Bargaining Agreement.

2. The Employer will provide opaque sleeves to unit employees for their PIV cards. The sleeves will meet National Institute of Standards and Technology standards for protection of electronic data on the cards.

3. When, in the process of applying for and receiving a PIV, an employee is informed that he or she will be required to undergo a background investigation, the Employer will inform the employee of the position sensitivity of their position and will provide (or provide a web link to) the appropriate forms that will be needed for the investigation. The forms will be appropriate to the sensitivity of the employee's position.

4. This agreement is effective on the date of the final signature below. Either party may reopen it at any time.

For the Union — Date: 4/7/08

For the Employer — Date: 4/4/08

For the Union — Date: 4/7/08

For the Employer — Date: 4/4/08