

**NORTHERN PLAINS AREA**  
**Policy Memorandum**

<b>DATE:</b>	March 14, 2008
<b>SUBJECT:</b>	Security at NPA Facilities
<b>NUMBER:</b>	PM-01-002
<b>EFFECTIVE DATE:</b>	Immediately Until Replaced or Superseded (Replaces PM-01-002 dated September 15, 2001)

**1. Purpose**

The safety and security of our employees, co-operators, and collaborators is of paramount importance to ARS; security of research projects and products is key to our mission; and the protection of our facilities is critical to the conduct of that research. This Memorandum describes basic requirements for physical security, and procedures for reporting suspicious activities and/or incidents at all facilities in the Northern Plains Area. It will be used in conjunction with other agency policy concerning the safety of employees and the security of our facilities. This guidance is not intended to be comprehensive, nor to replace sound judgment on the part of supervisors or managers.

**2. Occupant Emergency Plans**

Each research location will have a current Occupant Emergency Plan that details procedures to be employed and actions to be taken in response to emergencies. The plan will be developed in accordance with the guidance in ARS Policy and Procedure (P&P) 240.3, Physical Protection, Security, and Conduct While on ARS Controlled Property. The plan must be reviewed annually to ensure contact points and procedures are current and must be practiced at least once per year. A copy of the plan must be provided to each employee and to the Area Safety Manager.

**3. Business Continuity Plans**

Each location will have a current Business Continuity Plan that details how the location will operate during major events such as (flood, tornado, bird flu etc.). The plan should follow template provided by the Area Office. The plan must be reviewed annually to ensure contact points and procedures are current and must be tested on a regular basis. A copy of the plan must be on the NPA Security SharePoint site. Employees should be trained on the plan annually.

**4. Emergency Dismissals and Closures**

Generally, emergency dismissals and/or facility closures that require the use of administrative leave should be used when the facility is closed for the safety and security of personnel. The most common examples are weather emergencies or closure of the facility

for safety/health reasons such as plumbing or electrical failure. Only the head of the organization (Research Leader, Laboratory Director, Center Director, or person acting in that capacity) has the authority to close a facility and dismiss federal employees. Such a decision should be made in consultation with appropriate local officials, local Federal Executive Associations where they exist, and the Area Office if time permits. Dismissal of state or cooperator employees working at the facility should be coordinated with appropriate authorities or be in accordance with pre-arranged procedures. In an emergency situation, leaders should err on the side of caution for personnel safety and security. When notified of a Federal, Department, or Agency wide emergency closure, all employees are expected to depart the workplace after exercising assigned responsibilities for shut-down. In locally ordered closures or dismissals, leaders have broad discretion to determine a need for exigency employees to remain in or return to the facility.

## **5. Visitor Logs**

Each location will maintain a record of visitors to the facility, to include visiting scientists temporarily working in ARS laboratories or other research facilities. These records will consist of the date or duration of a visit, affiliation, company/department, vehicle license plate, who they are visiting, the citizenship of the visitor, and their date of birth. Group visits of students may be recorded as groups by the adult sponsor. Visitor logs must be maintained accurately, be retained indefinitely, and be in such order that they can be inspected by outside investigators. Foreign visitors must be reported in accordance with established procedures.

## **6. Reporting Security Incidents**

Locations will report any type of threatening or suspicious incidents to the Area Director's or Area Administrative office. Depending upon the nature and immediacy of the threat, other appropriate authorities, such as local law enforcement officers, should be summoned. All physical records, including e-mail or notes of telephone conversations, should be preserved for law enforcement officials. Employees should also be encouraged to report incidents which may be related to their employment but occur outside the workplace and/or during non-duty hours. Contact initiated by law enforcement officials, such as OIG, FBI, or local authorities should be reported to the Area Director's office.

## **7. Identification Cards and Badges**

Federal employees must be issued official employee identification with a picture and should display identification at all times while on the facility (ARS) premises. Locations may develop local identification badges for personnel authorized routine access to the facility. Access badges of this type should not reference or imply that the badge holder is an employee of ARS or the location. All identification cards must positively identify the individual, the status by which they are authorized to be on ARS property (federal, state, university, collaborator, or contractor), must include a picture of the badge holder, and must be numbered or otherwise accounted for in a recordkeeping system. Locations must maintain positive control of badges issued and require they be surrendered upon termination or when no longer needed. Visitors should be required to display a visitor pass

or badge while on the facility. Locations housed in University facilities must wear their Federal Id badges and are required to maintain records of individuals visiting ARS laboratories in these facilities.

Currently, Federal employees that have an appointment longer than 180 working days in either a single continuous appointment or a series of appointments will need a Personal Identity Verification (PIV) completed. An AD-1197 is filled out and submitted to HQ through the Area Human Resources Department. If approved by HQ, an official identification badge can be issued with a five year expiration for permanent Federal employees or for a temporary Federal employee a badge expiring on their NTE date. Until a PIV is approved by HQ, the location is responsible for issuing the Federal employee a provisional identification badge that initially expires 120 days of the EOD and can be extended in 30-day intervals until the AD-1197 is approved. **For more information on issuing identification badges and PIVs, please see P&P 243.4-ARS and Bulletin 07-411.**

ARS is in the process of implementing a Lincpass (smart card) to comply with Homeland Security Presidential Directive 12 (HSPD-12/2004) which requires the implementation of a government-wide standard for secure and reliable forms of identification. This will result in significant changes as Lincpass ID's will be issued via GSA Enrollment Centers. Information on the new protocol for issuing ID's to Federal employees, collaborators, and contractors will be forthcoming.

## **8. Facility Security**

New construction, modernization projects, and remodeling of facilities in the Northern Plains Area will include such standard basic security features as entry doors which are equipped with "swipe" or "proximity" card readers that are centrally controlled to record and limit access to office/laboratory complexes. Security lighting and fire suppressant features are also required. Additional appropriate protective measures must be determined locally based upon the level of risk to personnel and research products. Increased security requirements may be also determined in periodic security assessments conducted by the Agency or Area Office.

## **9. Security of Outbuildings, Plots, and Support Facilities**

Local security assessments will assist in determining the level of protection which may be necessary for outbuildings, above ground fuel storage tanks, utility areas, research plots, fields, and other types of structures or research sites which may support location research.

The nature and need for such protection should be based upon the exposure and the level of risk involved. Structures which may house chemicals or flammables should be protected by appropriate locks, fences, lighting, or other security features.

**10. Publications and Information**

Informational publications, including web sites, newsletters, brochures, and other materials, in printed, electronic, or other media, should not contain material that could attract adverse attention by radical groups. Those who prepare and approve such publications should seek guidance from the Area Office if questions arise concerning the sensitivity of such material. Currently, clear references to bioengineering projects, animal research, and similar topics should not be advertised to the general public.

**11. Responsibilities**

Research Leaders, Laboratory and Center Directors, and Administrative Officers are responsible for developing plans, communicating plans and procedures to employees, and ensuring that facilities are secured to the extent practicable under local conditions. These individuals are responsible for notifying the Area Office of any incidents or concerns regarding security issues, and for coordinating with local law enforcement officials to report criminal or suspicious activity.

**12. Point of Contact**

Questions concerning this policy or requests for waivers from this policy may be directed to the Area Administrative Office.

/s/

**W.H. BLACKBURN**  
**Area Director**  
**Northern Plains Area**