United States Department of Agriculture
Marketing and Regulatory Programs
Animal and Plant Health Inspection Service

Directive 1650.1 9/1/04

APHIS NATIONAL SECURITY PROGRAM

1. PURPOSE

a. This Directive establishes the APHIS National Security Program and provides guidance on operating procedures and responsibilities necessary to achieve an acceptable degree of security at all APHIS-owned and -leased facilities.

b. The APHIS National Security Program exists to mitigate loss, damage, or disruption of the APHIS mission. Homeland Defense and Presidential Decision Directives have mandated that Federal agencies take specific, and in some cases, extraordinary measures to protect employees, property, assets, and research from internal and external threats, both foreign and domestic. This Directive therefore establishes a National Security Team whose sole responsibility is to assess the current threats to APHIS, develop countermeasures to those threats, and coordinate implementation of those countermeasures.

2. REPLACEMENT HIGHLIGHTS

This Directive replaces APHIS Directive 1650.2, Security in Agency-Occupied Field Offices, dated 8/17/93, which contains outdated procedures for implementing security measures, issuing identification (ID) badges, and reporting thefts of Government property. This revision incorporates changes in regulations and clarifies actions needed to ensure implementation of the most recent security-related regulations and procedures for federally owned or leased facilities.

3. DEFINITIONS

a. Physical Security Assessments. A security site survey performed at APHIS facilities to determine specific security vulnerabilities and recommend appropriate security countermeasures.

b. Physical Security Countermeasures. Security deterrence measures implemented after a physical security assessment has been performed to mitigate vulnerabilities.

c. National Security Team. Members of the team assigned to the Director, Employees Services Division (ESD), MRPBS, having delegated responsibility for developing, implementing, and monitoring the Agency's physical security program on an Agencywide basis. Team members include the APHIS Security Officer, security specialists, and security assistants. In addition, other Agency and program security specialists and assistants (GS-0080 and GS-0086 series) with whom members of the team interact, and from/to whom advice and guidance is sought/provided, are also considered members of the National Security Team.

d. Restricted Areas. Areas within a facility requiring pre-determined access approval due to the existence of potentially hazardous materials, sensitive information or procedures, certain information technology (IT) equipment, or other high-value equipment

4. AUTHORITIES/REFERENCES

a. Department of Justice (DOJ) Vulnerability Assessment of Federal Facilities, dated June 28, 1995.

b. Department Regulation (DR) 1650-002, Building Safety/Security Occupant Emergency Program, dated 10/7/92.

c. USDA Integrated Physical Security Standards and Procedures Handbook, dated 11/14/03.

d. DR 9610-001, USDA Security Policies and Procedures for Bio-safety Level-3 Facilities, dated 8/30/2002.

5. POLICY

a. It is APHIS policy that the Department of Justice (DOJ) minimum-security standards for Federal facilities serve as a baseline for implementation of security standards and countermeasures at all APHIS-owned and -leased facilities. APHIS security considerations may supersede or override DOJ guidelines based on a threat at any particular facility. The DOJ "Vulnerability Assessment of Federal Facilities" Report dated June 28, 1995, established 52 minimum-security standards in five separate security levels. In addition to these standards, APHIS has considered additional Agency-specific factors, such as critical asset protection and essential mission capabilities, as essential ingredients in its security program.

b. Detailed guidance and procedures associated with various aspects of the APHIS National Security Program will be documented in the APHIS National Security Program Manual.

6. FACILITY SECURITY LEVELS

a. The complete DOJ Vulnerability Assessment of Federal Facilities can be viewed at: *http://www.oca.gsa.gov/dojreport.php.* Enter your Lotus Notes user name and password to access this report. Information about DOJ Security Levels is summarized in this Assessment.

b. Because of the diverse mission and size of APHIS facilities, each owned or leased facility is reviewed individually taking into account its unique mission, threat, crime, and surrounding environment. Based on these reviews, also called vulnerability assessments, different security measures are adopted at different facilities, ranging from a simple action like increased security lighting, to a contract action to obtain armed guards.

7. NATIONAL ACCESS CONTROL AND IDENTIFICATION BADGE SYSTEM

a. Establishment of a Nationwide Access Control and Badging System.

(1) The Agency has standardized and implemented the Lenel software as a national access control and badging system, which allows a single badge to work in all APHIS-controlled space. This system utilizes a single, proprietary system software and associated hardware. This system is nationally linked via the APHIS IT infrastructure and is managed and monitored by the APHIS Lenel Program Manager, a member of the National Security Team.

(2) Implementation of the Lenel system will gradually phase out individual program ID cards, as the Agency moves toward a “one Agency-one badge” process. ID badge procedures are established to safeguard sites, assets, and employees from criminal and terrorist threats.

(3) The APHIS Lenel Program Manager will designate subordinate Lenel Facility Representatives at each APHIS-owned and -leased facility that is brought online with the Nationwide Lenel Access Control and Badging System.

(4) Access control levels for employees may vary at each APHIS-owned and -leased facility. Authorized Issuing Officials (AIOs) are designated at all facilities. AIOs coordinate individual employee access with the APHIS Lenel Facility Representative.

b. Issuing and Wearing of ID Badges.

(1) ID badges are issued to all APHIS employees and contractors responsible for APHIS services. APHIS Form 511-R, ID/Access Request, ***http://www.aphis.usda.gov/library/forms/pdf/aph511.pdf*** will be used to document all individuals to whom ID cards are issued as well as to document access levels granted by authorizing officials. This form will be kept on record for 5 years. See Attachment 1.

(2) All APHIS employees and contractors will wear the APHIS-issued ID badge while in any APHIS-owned, -leased, or -occupied facility. The badge will be worn by chain or clip above the waist and in such a manner that it is visible at all times. Entry into the facility may be denied if persons refuse to show badges.

(3) Procedures for wearing ID badges can vary when working in mechanical shops or Bio-containment facilities; exemptions may be granted for safety or bio-security reasons. Procedures also may vary when employees are working around moving equipment, machinery, aircraft, animals, etc.

(4) Visitor ID badges will be issued to authorized visitors and will be returned when exiting the facility.

(5) APHIS ID cards will be issued for no longer than 5 years. When ID badges expire, APHIS Form 511-R will be resubmitted.

c. Replacement of Lost, Stolen, or Damaged ID Badges.

(1) Supervisors will submit APHIS Form 511-R to replace lost, stolen, or damaged badges. If the ID is lost or stolen, the supervisor will annotate the facts and the date of the occurrence on the form in the Remarks Section.

(2) For badges that are worn or damaged, supervisors need not submit APHIS Form 511-R if the original form remains on file.

d. Recovery of ID Badges.

(1) All employees will return their ID badge to their supervisor upon retirement, transfer, separation, or non-work status of a prolonged period.

(2) All supervisors will ensure that ID badges are returned to the appropriate Agency Lenel Facility Representative.

8. ESTABLISHMENT OF SECURITY MEASURES

In addition to the wearing of ID Badges, individual facilities may develop specific procedures to protect Government property from theft or damage. Some facilities may have restricted or critical areas to protect critical assets and infrastructures. Security measures for all other equipment must be dependent on the overall level of physical security for the particular office.

a. Security measures implemented in APHIS-owned and -leased facilities will be tailored to each location or site and the degree of security and control will depend on the nature, sensitivity, or importance of the security interest.

b. Restricted areas, such as where IT equipment that supports multiple offices is housed, where classified or sensitive information is used or stored, or where hazardous waste or high value equipment is housed, are afforded the highest level of security available, including, but not limited to: barriers, doors, high security locks, vaults, alarm monitoring, an intrusion detection system, closed circuit television surveillance, etc.

c. Admission of employees to a restricted area is granted to only those identified on an access control roster which is maintained by members of the National Security Team and the appropriate program managers at each APHIS-owned or –leased facility.

d. If an office environment is shared with another agency or it is a common building and APHIS employees do not control access, additional security measures to protect equipment may be necessary. Appropriate judgment should be exercised in determining the additional security measures to be implemented.

e. APHIS-owned or -leased space is to be used only for official business and authorized employee activities.

9. REPORTING THEFTS OR OTHER OFFENSES

a. Reportable offenses include theft of, or damage to, Government-owned or personally owned property or official records; break-in or attempted break-in at an APHIS-owned or -leased facility; vandalism, assault, disorderly conduct, or other criminal acts which occur in, or on the grounds of, Agency-occupied buildings or space. This includes offenses that occur in Government controlled, leased, or owned parking areas.

b. Employees will immediately report any of the above offenses to their immediate supervisor, or in the absence of the supervisor, to the next level of supervision.

c. Supervisors will immediately report any of the above offenses to the Federal Protective Service or the appropriate Building Manager, and, as appropriate, to local law enforcement authorities or members of the Office of the Inspector General. APHIS Form 515-R, Incident Report, ***http://www.aphis.usda.gov/library/forms/pdf/aph515.pdf*** will be used to document incidents and will be completed within 2 working days after the incident. See Attachment 2. Incidents also can be reported electronically. See: ***http://www.aphis.usda.gov/mrpbs/safety_security_national.shtml***

10. RESPONSIBILITIES

a. The APHIS Administrator will provide to Department and Congressional officials an explanation for program funding requests to implement the standards outlined in the DOJ "Vulnerability Assessment of Federal Facilities," dated June 28, 1995. Agency security specialists will provide the Administrator with documentation that explains the DOJ standards on which program-funding requests are based.

b. The Deputy Administrator, Marketing and Regulatory Programs-Business Services, has responsibility for the overall management of the APHIS National Security Program.

c. APHIS Program Deputy Administrators and Directors will:

(1) Ensure that all APHIS-owned or -leased facilities under their control have a designated official responsible for contacting their appropriate Agency security officer to ascertain security countermeasures needed at their respective facilities. This individual will serve as the focal point for physical security and will be delegated authority to coordinate countermeasures with Agency security specialists.

(2) Request the necessary funds to implement the security program within their respective organizations, as advised and directed by appropriate National Security Team members at the following offices:

(a) All offices in the Western Region and Building B, Ft. Collins, CO, call 970-494-7169.

(b) All offices in the Eastern Region and the AERO, Raleigh, NC, call 301-734-5662.

(c) Riverdale, MD offices, call 301-734-5662.

(3) Ensure that any security systems purchased are integrated into the nationwide Lenel Access Control and Badging System.

d. The Director, ESD, is responsible for the functional management of and leadership for, the APHIS National Security Program, and will:

(1) Develop, issue, and update security policy and procedures that are implemented consistently on an Agencywide basis.

(2) Coordinate with Directors of each APHIS-owned or -leased facility to ensure vulnerability assessments are conducted at their facility and plans generated to implement the recommendations of the assessment.

(3) Ensure that steps are put into place so that every Agency location meets, or has adopted plans to meet, minimum physical security standards, procedures, and protocols established by DOJ and/or by APHIS-contracted or -provided security assessments.

(4) Coordinate with Directors of each APHIS-owned or -leased facility to establish procedures that successfully implement guidelines of the security program.

e. Directors of each APHIS-Owned or -Leased Facility will:

(1) Advise their respective Deputy Administrator and members of the National Security Team when security assessment activities reveal situations requiring immediate corrective action.

(2) Keep National Security Team members informed of any threats directed against APHIS-owned or -leased facilities and their employees, as well as the capabilities and limitations of the facility security program to counter such activities.

(3) Contact National Security Team members with any concerns or questions about procedures for ID Badging and the necessity of obtaining security guards.

(4) Consult with members of the National Security Team prior to any installation of any security equipment, so that the required standards can be assessed.

f. The Director, Administrative Services Division, is responsible for:

(1) Ensuring that appropriate Architecture/Engineering employees contact ESD security specialists to review and provide input to building specifications before any construction contracts are awarded, in order to ensure expensive retrofitting is not required.

(2) Ensuring procurement officials contact a representative of the National Security Team before purchasing items such as: closed circuit TV, alarm systems, fencing, guard services, etc. The National Security Team must be apprised of security vulnerabilities in order to ensure that appropriate countermeasures are being procured.

g. The Director, IT Division, is responsible for ensuring that members of the National Security Team are provided the required IT technical and customer assistance and support to implement the Lenel Access Control and Badging System. IT Customer Service Branch employees and National Security team members must coordinate to ensure both IT and security-related needs are addressed as additional locations throughout the country are brought online.

h. The National Security Team:

(1) Serves as the focal point for all physical security purchases, guard and security system contracts, and implementation of security measures within APHIS.

(2) Develops internal Agency policies to ensure the Agency's compliance with minimum security standards developed by the DOJ, and documents security related procedural guidelines in the APHIS National Security Program Manual.

(3) Assists in the implementation of minimum-security standards and countermeasures in all APHIS offices.

(4) Administers the nationwide Lenel Access Control and Badging System in cooperation with IT employees.

(5) Consults with IT and Emergency Operations employees on all physical security and access control issues that impact IT, Cyber, or Information Security.

(6) Provides educational material as it relates to security and building emergencies.

(7) Provides advice, guidance, and approval for the purchase of items such as closed circuit TV, alarm systems, fencing, etc., as well as technical assistance in the implementation and installation of security systems in APHIS occupied spaces (leased or owned).

(8) Researches, plans, develops, and implements security strategies and budgets from a program and/or Agency level.

i. Supervisors and Managers are responsible for:

(1) Enforcing security procedures outlined in this Directive.

(2) Following up with appropriate security employees when security discrepancies have been reported to them.

(3) Ensuring corrective action is taken when security assessment activities reveal deficiencies.

j. All APHIS Employees and APHIS Contract Employees will:

(1) Follow all procedures in this Directive pertaining to ID badges. At no time are ID badges to be loaned or borrowed.

(2) Report to their immediate supervisor any security-related concerns they may have or any security discrepancies they may observe in their working environment.

(3) Allow physical inspection or x-ray of items carried into any APHIS-owned, -leased, or -occupied facility.

(4) Limit access to working areas by non-authorized persons.

11. INQUIRIES

a. Direct inquiries regarding the APHIS National Security Program to the offices listed in Section 9.c. 2. (a) through (c).

b. This Directive is available on the APHIS Employee Library website at ***www.aphis.usda.gov/library***

c. Additional information pertaining to the APHIS National Security Program can be found at ***http://www.aphis.usda.gov/mrpbs/safety_security_national.shtml***

/s/
William J. Hudnall
Deputy Administrator
MRP Business Services

2 Attachments