

For: State and County Offices

USDA Nationwide Security Survey

Approved by: Deputy Administrator, Management



1 Overview

A Background

In coordination with the Homeland Security Presidential Directive-12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors”, USDA, Office of Operations, Physical Security Office is conducting a nationwide physical security on-line survey to produce a program baseline and a facility inventory of existing security equipment at all USDA facilities nationwide.

B Purpose

This notice advises all State and County Offices to complete the Pre-Survey Checklist (Exhibit 1) and the On-Line Survey for each office location, which includes shared management offices and part-time offices, by COB February 15, 2006.

Note: Other USDA agencies located in the same building will also be completing the same survey.

C Contact

If there are any questions about this notice:

- County Offices shall contact the State Office
- State Offices shall contact Walter “Skip” Mielwocki by either of the following:
 - e-mail at **Skip.Mielwocki@wdc.usda.gov**
 - telephone at 202-720-9395.

Disposal Date	Distribution
April 1, 2006 1-23-06	State Offices; State Offices relay to County Offices

Notice AO-1348

2 Data Call

A Receiving the Data Call

The information contained in the On-Line Survey will assist USDA to prioritize and implement a transition plan for all USDA facilities to be compliant with OMB's requirements for HSPD-12.

3 Exhibits

A Pre-Survey Checklist

The Pre-Survey Checklist (Exhibit 1) is designed to guide the survey reporter in gathering the information necessary to complete the online version of the USDA HSPD-12/FIPS 201 Physical Security Systems data call. The information contained in the Pre-Survey Checklist will be the same information that is input into the On-Line Survey.

Note: After the On-Line Survey has been completed, maintain the Pre-Survey Checklist in a temporary file for 180 calendar days.

B Definitions

Exhibit 2 contains definitions of the terminology used in the Pre-Survey Checklist. The term "affiliates" is used in the pre-survey checklist, but is not defined in the list of definitions. For HSPD-12 purposes, the term affiliate is defined as non-Title 5 employees. Affiliates include non-Federal permanent (CO grade) employees.

4 Action

A State and County Office Action

Each State and County Office shall input the respective data after first completing the Pre-Survey Checklist at <http://extsurvey.bah.com/2way/2w90W4/Link.html>.

Note: The password is "ffassurvey1".

B Additional Instructions for the Pre-Survey Checklist

Number	Description	Action
1	Contact Information	Use: <ul style="list-style-type: none">• AO information for State Offices• CED information for County Offices.
3	Full Time Employees (FTE's)	County only full-time permanent GS employees.
	Affiliates	County full time permanent CO employees. Do not include COC members, temporary employees, and student interns.

Pre-Survey Checklist

 UNITED STATES DEPARTMENT OF AGRICULTURE		PRE-SURVEY CHECKLIST		
Physical Security Systems Data Call		<i>Purpose:</i> The Pre-Survey Checklist is designed to guide survey reporters to gather the information necessary to complete the Web-based version of the USDA HSPD-12/FIPS 201 Physical Security Systems data call. <i>Directions:</i> Fill in the checklist blanks and use the checklist to complete the survey.		
Task to be Accomplished / Information to be Gathered	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
1. Be prepared to identify yourself, your contact information, your position/title, and the unit/section/division and address you are reporting on.				
2. If you are reporting on more than one facility or need to report on more than one location, you should be prepared to provide that information. <i>Note: The survey will permit you to enter the data for one facility at a time. You will be able to stop and resume the survey at any point.</i>				
3. Know the following information regarding the population of the facility you are reporting on. <ul style="list-style-type: none"> • Number of Full Time Employees (FTEs) • Number of Contractors • Number of Affiliates 				
4. Determine which of the following best describes the type of facility/property you are reporting on. <ul style="list-style-type: none"> • Leased building or property (USDA or GSA Owned or Other) • Government owned facility and property (Government only - no tenants or non-government occupants) • Multiple Tenant location (including non-government agencies or occupants) which is owned or leased by the USDA • Multiple Tenant location (including non-government agencies or 				

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

Pre-Survey Checklist (Continued)

Task to be Accomplished / Information to be Gathered occupants) in which the USDA is considered a tenant (i.e. university setting) • Other (please describe)	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
5. Determine if personnel at this facility are required to wear Government-issued Identification cards or credentials as a prerequisite to gain access to the location you are reporting on. <i>Note: If ID media is required for access you will also need to determine if there is a person, such as a receptionist or security officer tasked with the responsibility of checking credentials.</i>				
6. Ascertain whether or not the facility you are reporting on utilizes an electronic security system (intrusion detection system) for access control. <i>(Refer to the data call definition list to assist you with nomenclature)</i> <i>(If the answer is NO, please skip to Question18)</i>				
<ul style="list-style-type: none"> • If yes, you will be asked to identify the following: <ul style="list-style-type: none"> ○ The number of doors equipped with mechanical door locks and keys at this facility ○ The number of doors equipped with mechanical combination or cipher-locks and keys at this facility ○ Each type of electronic security component being used to gain access at the facility you are reporting on: <ul style="list-style-type: none"> ▪ Magnetic Strip (swipe) Card Reader ▪ Proximity Card Reader ▪ Key fob ▪ Radio Frequency Identification (RFID) ▪ Personal Identification Number (P.I.N.) Key Pad ▪ Biometrics Fingerprint - Optical ▪ Biometrics Fingerprint - Capacitive ▪ Biometrics - Hand Geometry ▪ Biometrics - Iris Scan 				

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

Pre-Survey Checklist (Continued)

Task to be Accomplished / Information to be Gathered	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
<ul style="list-style-type: none"> ▪ Biometrics - Retina Scan 				
<ul style="list-style-type: none"> ▪ Biometrics - Face Scan 				
<ul style="list-style-type: none"> ▪ Biometrics - Voice Print 				
<ul style="list-style-type: none"> ▪ Biometrics - Signature 				
7. Determine if this facility has Alarm Assessment Capability.				
8. Determine if this facility utilizes an Alarm Communication and Display function.				
9. Determine if the facility has physical access delay measures in place (i.e., double doors, mantrap, etc.)				
10. Ascertain if the facility utilizes Intrusion Detection Equipment not previously described. <i>(Please be prepared to explain)</i>				
11. Determine if this facility utilizes integrated Closed Circuit Television (CCTV) or Video Assessment Systems in conjunction with access controls.				
12. Determine the total number of access control points (where employees, visitors, contractors are permitted to enter a facility) for the facility you are reporting on.				
13. Determine the name brand of the head-end software (software that runs the security system) and the version being used (e.g., Lenel v. 2.1) for the facility you are reporting on.				
14. Identify the control signals (the methods used to send signal and control data, e.g. the wiring to connect the system) used for this facility from the following: <ul style="list-style-type: none"> • Wire (metallic cable with insulation) 				

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

Pre-Survey Checklist (Continued)

Task to be Accomplished/ Information to be Gathered	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
<ul style="list-style-type: none"> • Coaxial cable • Fiber Optic cable (with protective outer jacket) • RF (Radio Frequency Wave) • Wireless 				
15. Determine whether the facility owns or leases it's access control system.				
16. If the facility access control system is leased from a vendor, determine if the facility's access control system tied into the lease-provided system.				
17. Determine the kind of connectivity that the facility's access control system has with the computer network of the facility/location.				
<ul style="list-style-type: none"> • Web access VPN • Local Area Network Drop • T1 Line • T3 Line • Extends to IP line external to the facility • Dial Up Connection • Broadband Connection • Don't Know 				
18. Determine whether or not the facility you are reporting on produce and issue its own credentials (badges).				
<ul style="list-style-type: none"> • <i>If no, please go on to the next question</i> • If yes, please be prepared to specify the Office and Point of Contact (name, telephone number, email address) of the person/office that produces credentials/badges for your facility/location. Answer the following questions: <ul style="list-style-type: none"> ○ How many ID cards (credentials have been produced at this facility over the history of the facility? 				

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

Pre-Survey Checklist (Continued)

Task to be Accomplished / Information to be Gathered	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
<ul style="list-style-type: none"> ○ Briefly explain how the credentials are produced (what system and what method). ○ Is the facility equipped with an electronic registration station to produce the credentials? 				
<p>19. Be prepared to indicate the number of Federal employees or Federal contractors would need a new PIV compliant ID card at the location you are reporting on.</p>				
<p>20. Determine where the information is currently stored for each ID cardholder. Is the information stored in:</p>				
<ul style="list-style-type: none"> • Database files 				
<ul style="list-style-type: none"> • Text files 				
<ul style="list-style-type: none"> • Floppy disk 				
<ul style="list-style-type: none"> • Removable hard drive 				
<ul style="list-style-type: none"> • Hard copy (paper) 				
<ul style="list-style-type: none"> • Other (please explain) 				
<p>21. Determine what safeguards (locking fireproof filing cabinet, passwords, etc.) are used to protect this information.</p>				
<p>22. Determine and be prepared to describe the standard topology for the ID card issued to each employee/contractor (e.g., computer generated, preprinted form, etc.).</p>				
<p>23. Ascertain of contractors receive the same type of ID card as regular Federal employees. If not, please be prepared to explain the difference.</p>				
<p>24. Determine whether or not the facility you are reporting on is a location which currently utilizes Smart Cards (multi-technology, approved Federal Identity Credentialing Committee (FICC) topology, or other).</p>				

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

Pre-Survey Checklist (Continued)

Task to be Accomplished/ Information to be Gathered	✓ YES	✓ NO	✓ N/A	Comments/Notes/Quantities
25. Determine if the facility you are reporting on has implementation plans currently being executed, in progress, or planned which would facilitate the use of Smart Cards for access control at this location. (Please describe budget completed, equipment purchases, implementation has begun, etc.)				END OF CHECKLIST

USDA HSPD-12/FIPS 201 Pre-Survey Checklist

6

Definitions

DEFINITIONS

Access Controls. Access controls regulate the flow of people, vehicles, and resources into, out of, and within a protected facility. Access controls are often employed as a means of protecting assets and they also facilitate the important role of controlling the movement (or circulation) of personnel in and around a facility requiring protection. Access is also the process of granting or denying specific requests such as: (1) obtaining and using information and related information processing services; and (2) entering specific physical facilities (i.e., Federal buildings, military establishments, border crossings, etc.). (*Department of Commerce, National Institute of Standards and Technology, FIPS PUB 201, 2005*)

Access Control System. A typical functioning access control system will consist of card readers, proximity or swipe cards, door position switches, automatic door lock/release mechanisms, door closures, system software, network components, battery back-up for the system's control panel and each access door, cabling, output/control delays, printer, documentation and other associated equipment and materials. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Access Delay Measures. An effective security system requires that any malevolent act committed by an inside or outside adversary must be detected so that the response force, including on-site guards, local police, and others, can interrupt the adversary's attack before the goal is achieved. The performance measure for access delay is time. Delay time for the adversary will depend on the barrier to be breached and the tools to be used. Delay elements include passive barriers, guards, and dispensable barriers. As part of protection-in-depth, delay-in-depth should be implemented. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Agency. Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of Government. (*Federal Identity Management Handbook, 2005*)

Alarm Assessment Capability. The process of determining an alarm condition status based upon the importance or seriousness of the alarm, then determining an alarm condition status and assessing the credibility, reliability, accuracy, and usefulness of an indicated alarm associated with an access control sensor. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Alarm Communication and Display (AC&D). AC&D refers to the integrated system of people, procedures, and equipment that collects alarm data and presents the information in a manner that promotes rapid assessment. The

Definitions (Continued)

communications subsystem transfers data from one physical location to another (i.e., from the collection point such as sensors to a central repository known as the display). The central repository may consist of multiple computers or displays. If a sensor activates, the alarm communications system must assure that accurate data pertaining to the activation is received. As a result, assured message delivery means the communication system must be reliable. The physical layer of AC&D provides mechanical, electrical, functional, and procedural methods used to transmit information from one place to another. In turn, the network layer provides addressing, sequencing, flow-control, receipt/acknowledgement, and error-handling services. The network layer takes higher-level data and packages it for transmission. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Asset Protection. Normally, physical and intellectual property, money, and proprietary information are considered types of assets worthy of protection. The employees of an organization should also be considered among the enterprise's most valuable assets. Without a trained work force to do the work, other assets may be useless to the organization's mission or business. (*Protection of Assets, 2000*)

Biometric. Defined by the National Institute of Standards and Technology Federal Information Processing Standards Publication 201 as a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity of an applicant or person requesting access. Facial images, fingerprints, and iris-scan samples are examples of biometrics. (*Department of Commerce, FIPS PUB 201, 2005*)

Biometrics Face Scan. Facial verification systems are distinguishing characteristics of the face to verify a person's identity. Most systems capture the image of the face using a video camera, although one system captures a thermal image using an infrared imager. Distinguishing features are extracted from the image and compared with previously stored features. If the two match within a specified tolerance, positive identity verification results. Although facial systems have been proposed and studied for several years, commercial systems have only been available recently. (*Effective Physical Security, 2004*)

Biometrics Fingerprint - Capacitive. Most fingerprint verification systems use minutia points, the fingerprint ridge endings and bifurcations, as the identifying features of the fingerprint, although some systems use the whole image for comparison purposes. Direct imaging sensors using solid-state devices such as capacitive or thermal methods have been commercially developed and may be procured at a relatively lower cost due to the efficient manufacture of silicon chips. (*Effective Physical Security, 2004*)

Definitions (Continued)

Biometrics Fingerprint – Optical. Optical methods of fingerprinting use a prism and a solid-state camera to capture the fingerprints. (*Effective Physical Security, 2004*)

Biometrics Hand Geometry. Personnel identity verification using the hand geometry system is based on characterizing the shape of the hand. The underlying technique measures three-dimensional features of the hand such as the widths and lengths of fingers and the thickness of the hand. During verification the feature vector is compared with previous measurements (the template) obtained during enrollment. If the feature vector and template match within an allowable tolerance, verification is successful. (*Effective Physical Security, 2004*)

Biometric Information. The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristics (e.g. patterns). (*Federal Identity Management Handbook, 2005*)

Biometrics Iris Scan. Similar to the retinal scan, another technology uses the iris to accomplish identification. The iris is the colored portion of the eye that limits the amount of light allowed into the eye. The system uses a video camera to image the iris structure of the eye. The unique structure of the iris can be used to identify an individual. (*Effective Physical Security, 2004*)

Biometrics Retinal Scan. The retina is the membrane lining the more posterior part of the inside of the eye. It contains light-sensitive cones and nerve cells. The pattern of blood vessels in the body is unique, and the pattern on the retina of the eye can be assessed optically through the lens of the eye. The retinal scanner can also operate in the recognition mode. (*Effective Physical Security, 2004*)

Biometrics Signature. Handwriting verification has been used for many years by the banking industry. Handwriting verification systems have been developed that use handwriting dynamics, such as displacement, velocity, and acceleration. Statistical evaluation of these data indicates that an individual's signature is unique and reasonably consistent from one signature to the next. These systems generally provide low security and are best used in applications where authorizing signatures for a transaction are already in use. (*Effective Physical Security, 2004*)

Biometrics Voice Print. Voice is a attribute which can be used to verify identity. Speech measurements useful for speaker discrimination include waveform envelope, voice pitch period, relative amplitude spectrum, and resonant

Definitions (Continued)

frequencies of the voice tract. The system may ask the user to speak a specific predetermined word or to repeat a series of words or numbers selected by the system in order to verify access. While this technology currently offers relatively low security, it is an attractive alternative due to its ease of deployment and acceptance by the public. (*Effective Physical Security, 2004*)

Cardholder. An individual possessing an issued PIV card. (*Federal Identity Management Handbook, 2005*)

Card reader. Equipment capable of reading the information on a card such as that in the magnetic strip or chip. (*Federal Identity Management Handbook, 2005*)

Card printer. Equipment capable of printing information on the physical surface of the card. (*Federal Identity Management Handbook, 2005*)

Closed Circuit Television. CCTV is a reliable, cost effective deterrent and a means for apprehension and prosecution of offenders. Although the main objective of a properly designed and installed CCTV should not be the apprehension of thieves, but, rather the deterrence through security so as to prevent criminal activity. CCTV is effectively integrated with other sensing systems (alarms) and its use to view remote areas having potential security and safety problems, or fire hazards. (*Effective Physical Security, 2004*)

Coaxial cable. A cable (also known as a coax) consisting of single conductor surrounded by, and insulated from, metallic shield, used for the transmission of video baseband and high-frequency signals. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Control Signals. Required for the operation of access control devices since data and communications are required to detect and annunciate alarms. (*Effective Physical Security, 2004*)

Credential. Evidence attesting to one's right to credit or authority. As associated with the PIV standard, credential refers to the PIV card and the data elements connected with an individual that authoritatively binds an identity to that individual. (*Department of Commerce, FIPS PUB 201, 2005*)

Fiber optic cable. Fiber optics is the preferred leading edge technology for data transmission. Fiber optics permits long distance connections with very good reliability. (*Effective Physical Security, 2004*)

Federal Identity Credentialing Committee approved card topology. The mandatory elements on an approved PIV card include: the photograph of the

Definitions (Continued)

PIV cardholder on the front of the card; the name of the PIV cardholder on the front of the card; the employee affiliation of the PIV cardholder on the front of the card; the name of the agency, department, and/or organization with which the PIV cardholder is affiliated on the front of the card; the expiration date of the PIV card on the front of the card; the agency card serial number of the back of the card; and the issuer identification on the back of the card. (*Federal Identity Management Handbook, 2005*)

Federal Information Processing Standard Publication 201 (FIPS 201).

Published by the Department of Commerce and the National Institute of Standards and Technology, the FIPS 201 specifies specifications on Federal physical access control systems (PACS) and describes how the Personal Identity Verification Card should be used in PACS throughout the Federal Government. FIPS 201 consists of two parts: PIV I and PIV II. The standards in PIV I support the control objectives and security requirements described in HSPD-12. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II also specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards for use in the Federal PIV system). (*Smart Card Alliance, September 2005*)

Head end access control software. Leading edge access control technology is integrated with leading headend software which allows administrators to centrally manage access to virtually any location - wired or standalone - as well as receive comprehensive audit logs for all access points. In effect, each card or smart credential securely carries the roles and privileges of the individual from wired to standalone access points, creating a card-connected environment. In this way, within a software-enabled access control system, cardholders become an extension of the physical access network, and their cards carry information to and from the readers. By following this model, security is increased significantly at a fraction of the normal cost. (*Smart Card Alliance, September 2005*)

Homeland Security Presidential Directive -12 (HSPD-12). HSPD-12 identifies the *Policy for a Common Identification Standard for Federal Employees and Contractors*. The Directive promulgates a Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). The purpose of the policy is to enhance security, increase Government efficiency, reduce identity fraud, and to protect personal privacy. (*HSPD-12, August 2004*)

Identification. The process of discovering the true identity (the set of physical and behavioral characteristics by which an individual is uniquely recognizable) of a person or item from the entire collection of similar persons or items in a data warehouse. (*Department of Commerce, FIPS PUB 201, 2005*)

Definitions (Continued)

Identity Management System (IDMS). Identity management system comprised of one or more systems or applications that manages the identity verification, validation and issuance process. (*Department of Commerce, FIPS PUB 201, 2005*)

Identity Verification. The process of confirming or denying that a claimed identity is correct by comparing the credentials (*something you know, something you have, something you are*) of a person requesting access with those previously proven and stored in a PIV card or system and associated with the identity being claimed. (*Department of Commerce, FIPS PUB 201, 2005*)

Interoperability. The standard that permits any government facility or information system to verify a cardholder's identity using the credentials provided on the PIV card. (*Department of Commerce, FIPS PUB 201, 2005*)

Intrusion Detection Systems/Equipment. Intrusion detection systems and equipment are a set of technologies that define, observe, control, and sense entry into a defined controlled or secure area. (*Effective Physical Security, 2004*)

Key Fob. Designed to be attached to or part of a standard key ring, the key fob is similar to a proximity access card in operation. This technology uses a contactless interface with a card reader. The antenna is embedded in the card, which emits a unique radio frequency when in close proximity to the electronic field of the card reader. (*Effective Physical Security, 2004*)

Logical Access Control Systems (LACS). An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability of assigning different access control privileges to different persons depending upon their roles and responsibilities in an organization. (*Federal Identity Management Handbook, 2005*) The access controls associated with USDA information systems and computing resources. (*USDA Draft HSPD-12 Implementation Plan, June 2005*)

Mantrap (secure vestibule). Mantraps, otherwise known as double vestibule hall portals, are used to unobtrusively examine visitors prior to admission, keep nonconforming people out, and make sure that two people do not enter at one time (piggybacking) when entering or leaving a building. (*Effective Physical Security, 2004*)

Magnetic Strip (swipe) Card Reader. This type of card has a data-encoded stripe on one face. When the card is withdrawn from, or swiped through a

Definitions (Continued)

reader, the stripe passes over a magnetic head not unlike that of a tape player. Access criteria reflect the cardholder's identity, the areas the cardholder is authorized to enter, and time frames for entry. Compared to other card types, stripe cards cost less and can hold a large amount of data, however, the magnetic stripe can wear out or become damaged over time. (*Effective Physical Security, 2004*)

Mechanical combination lock (cipher lock). This type of lock permits the combination of the lock to be changed for higher security. Unlike the electronic combination lock or keypad, there is not electrical power required. A key insert is required to change the combination. (*Effective Physical Security, 2004*)

Mechanical door lock. A key operated mechanical lock uses some sort of arrangement of internal physical barriers (wards, tumblers) which prevent the lock from operating unless they are properly aligned. The lock itself is normally permanently installed. The key is considered a separate piece, which is designed for removal from the lock to prevent its unauthorized use. The mechanical door lock is very mature technology and electrical power is normally not required. (*Effective Physical Security, 2004*)

National Agency Check and Inquiries (NACI). The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (with inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). (*Department of Commerce, FIPS PUB 201, 2005*)

Personal Identification Number (P.I.N.) Keypad. Similar to an electronic combination lock, this keypad is programmable and electrical power is required. Generally, the use of a keypad provides another layer of access control in addition to a key or card reader. The drawbacks of a standard P.I.N. keypad are: the combination code is hard to secure and there is little trace ability to determine who has opened the lock/device. (*Effective Physical Security, 2004*)

Personal Identity Verification (PIV). HSPD-12 requires that the Federal credential (the PIV card) be secure and reliable, which is defined as a credential that: is issued based on sound criteria for verifying an individual's identity; is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; can be rapidly authenticated electronically; and, is issued only by providers whose reliability has been established by an official accreditation process. (*Smart Card Alliance, September 2005*)

Definitions (Continued)

PIV Card. The PIV Card stores a cardholder photograph, cryptographic keys, biometric data and the cardholder unique identifier (CHUID). The card allows the identity of the cardholder to be verified. Typically, the card is presented to a card reader to initiate an authentication transaction and to request access authorization. Also known as a “smart card” issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable) or an automated process (computer readable and verifiable). (*Department of Commerce, FIPS PUB 201, 2005*)

Physical Access Control System (PACS) Requirements. A Physical Access Control System has many benefits including enhancing the security for personnel entering, leaving, or working within a facility. A typical FIPS 201-compliant PACS contains the following components: PIV Card; PIV Card Reader; Biometric Reader; Control Panel; Access control server, cardholder data repository, and control points. (*Smart Card Alliance, September 2005*)

Physical security. The use of people, procedures and equipment (alone or in combination) to control access to assets or facilities; the measures required for protection of assets or facilities from espionage, theft, fraud, or sabotage by a malevolent human adversary. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Proximity Card Reader. Refers to a technology used to provide physical access control. This technology uses a contactless interface with a card reader. The antenna is embedded in the card, which emits a unique radio frequency when in close proximity to the electronic field of the card reader. (*Effective Physical Security, 2004*)

Radio Frequency Identification (RFID). RFID uses low-powered radio transmitters to read data stored in a transponder (tag) at distances ranging from 1 inch to approximately 100 feet. RFID tags are used to track assets, manage inventory and authorize payments, and they increasingly serve as electronic keys for everything from autos to secure facilities. (*Effective Physical Security, 2004*)

Secure and Reliable Communications. Defined by HSPD-12 to mean the identification that: (a) is issued based on sound criteria for verifying an individual employee’s identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. (*HSPD-12*)

Definitions (Continued)

Standard. A published statement on a topic specifying the characteristics that must be satisfied or achieved to comply with the standard. (*Department of Commerce, FIPS PUB 201, 2005*)

Twisted pair. A two-conductor transmission line seldom used in video systems due to limited distance and bandwidth capabilities. (*The Design and Evaluation of Physical Protection Systems, 2001*)

Wire (metallic cable with insulation). The least inexpensive cabling necessary for data and power transmission required for access control systems. The easiest cable to install and connect. However, standard wire cable is limited to shorter distances than fiber optics and are subject to electromagnetic interference. (*Effective Physical Security, 2004*)

Wireless. Wireless alarm/sensor systems are easily expandable and easily installed because they require no wires. (*Effective Physical Security, 2004*)