U.S. Customs and
Border Protection

Attachment Z

Terms and Definitions and Acronyms

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	July 27, 2009	Initial Release
2.0	December 21, 2010	No changes.

CONTENTS

1.0 Terms and Definitions

Terms and definitions in this section are provided to aid users in understanding essential security concepts presented in this policy handbook. Such terms are fundamental to the policies outlined in this document. Other definitions may be found in the National InfoSec Glossary (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf), as well as the Privacy Incident Handling Guidance and the Privacy Compliance documentation located at http://www.dhs.gov/Privacy.

Availability – timely, reliable access to data and information services for authorized users.

Certification Authority – (for PKI) binds the identity of the subscriber to his/her public key by issuing a digital certificate signed by the Certification Authority containing the distinguished name of the subscriber and the subscriber's public key.

Classified National Security Information – Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Common Criteria – provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (International Standard ISO/IEC 5408, Common Criteria for Information Technology Security Evaluation [ITSEC])

Confidentiality – ensures that information is disclosed only to those who are authorized to view it.

Continuity of Operations- Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that: delineate essential functions and supporting IT systems; specify succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications; and validate the capability through tests, training, and exercises.

Continuity of Operations Plan- A plan that provides for the continuity of essential functions of an organization in the event that an emergency prevents occupancy of its primary facility. It provides the organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility.

Cryptography – a branch of mathematics that deals with the transformation of ordinary text (plaintext) into coded form (cipher text) by encryption and the reverse operation, decryption, which is the transformation of cipher text into plaintext.

Data Owner – the entity having responsibility and authority for the data.

Denial of Service (DoS) – an attack characterized by the explicit attempt to prevent legitimate users from using a service. Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Examples of DoS include:

- Attempt to “flood” a network, thereby preventing legitimate network traffic
- Attempt to disrupt connections between two machines, thereby preventing access to a service
- Attempt to disrupt service to a specific system or person
- Attempt to prevent a particular individual from accessing a service

DHS IT System- A DHS system is any IT that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include general support systems and major applications.

Digital Certificate – a digital document that attests to the truth that you are who you say you are, and that you own the particular public key specified in the certificate.

Eavesdropping – a method of attack against the confidentiality of data transmitted across the network. In a wireless network, eavesdropping is the most significant threat because an attacker can intercept the transmission over the air from a distance away.

Essential Functions- Functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial/economic base during an emergency.

Federal Information Security Management Act (FISMA)- The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide a high-level of security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Statutory requirements include:

(1) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

(2) Policies and procedures that:

   a. Are based on the risk assessments required by paragraph (1) above

   b. Cost-effectively reduce information security risks to an acceptable level

   c. Ensure that information security is addressed throughout the life cycle of each agency information system

   d. Ensure compliance with

i. Other federal policies and procedures as may be prescribed by OMB and NIST, or other agencies when appropriate

ii. Minimally acceptable system configuration requirements, as determined by the agency

iii. Any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President

(3) Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) Security awareness training to inform personnel, including contractors and other users of information systems that support operations and assets of the Department, of:

a. Information security risks associated with their activities

b. Their responsibilities in complying with agency policies and procedures designed to reduce these risks

(5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing:

a. Shall include testing of management, operational, and technical controls of every information system identified in the Department's inventory

b. May include testing relied on by the Office of Inspector General;

(6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the Department

(7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines promulgated by USCERT

a. Mitigating risks associated with incidents before substantial damage is done

b. Notifying and consulting with the USCERT

c. Notifying and consulting with:

i. Law enforcement agencies and relevant Offices of Inspector General

ii. An office designated by the President for any incident involving a national security system

iii. Other agency or offices, as required

(8) Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the Department

FISMA requires the Chief Information Officer to designate a senior agency information security official who shall develop and maintain a Department-wide information security program as required by the statute. Responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements

- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities
- Assisting senior Department officials concerning their responsibilities under the statute
- Ensuring that the Department has trained personnel sufficient to assist the Department in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
- Ensuring that the Department Chief Information Officer, in coordination with other senior Department officials, reports annually to the Department head on the effectiveness of the Department information security program, including progress of remedial actions.

Foreign Intelligence Information – information that relates to the capabilities, intentions and activities of foreign powers, organizations or persons, but does not include counterintelligence, except for information on international terrorist activities.

General Support System (GSS) – is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, applications, communications, data and users. Examples of a GSS include a local area network (LAN), including smart terminals that support a branch office, an agency-wide backbone, a communications network, or a departmental data processing center including its operating system and utilities.

Note: GSS shall be under the direct oversight of the CISO, with support from the SOC. All general support systems must have one or more Information Systems Security Officers (ISSO) assigned.

Information Assurance (IA) –protect information systems and data by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating a protection, detection, and reaction capability.

Information Technology – (per the Clinger-Cohen Act) any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.

Information Type – a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity – ensures that information has not been altered accidentally or deliberately, and that it is accurate and complete.

Intranet – a web communications system established within the limited confines of a given enterprise, such as a network internal to a given business or agency.

Least Privilege – principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error or unauthorized use of an information system.

Major Application – A major application (MA) is an automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each major application must be under the direct oversight of a CISO and must have one or more Information Systems Security Officers (ISSO) assigned.

Malicious Code – a computer program or part of a computer program, designed to take an action that, if the end user knew about, s/he would not permit to happen, such as deletion of an entire hard disk. Although the terms, "virus" and "malicious code" have become interchangeable, not all instances of malicious code are technically viruses and not all viruses constitute malicious code.

Management Controls – focus on managing both the system IT security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

National Security Information – Information that has been determined, pursuant to Executive Order 12958 (as amended) or any predecessor order, to require protection against unauthorized disclosure.

Non-Repudiation – assurance that sender and recipient identities of a message are provided so that neither can later deny having possessed the data.

Operational Data- Operational data is information used in the execution of any CBP mission.

Personal Digital Assistant – a handheld device that combines computing, telephone/fax, Internet and networking features.

Protection Profile – common criteria specification that represents an implementation-independent set of security requirements for a category of Target of Evaluations that meets specific consumer needs.

Risk – possibility of loss or injury, the degree of probably of such loss, and the adverse impact on achieving organizational objectives. Risk level is categorized by severity of impact and probability of occurrence.

Risk Assessment – the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets or individuals by determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact.

Part of risk management is synonymous with risk analysis and incorporates threat and vulnerability analysis.

Sanitization – the process used to remove information from media such that data recover is not possible. It includes removing all classified labels, markings, and activity logs.

Security Appliance – hardware, software, firmware, or combination device that provides a security service or countermeasure against a particular exploit. Examples would include firewalls, VPNs, remote access smartcards, encryptors, Internet gateways, and video surveillance devices.

Security Category – the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational assets or individuals.

Security Controls – management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Policy – rules and practices that regulate how a system or organization protects sensitive and critical system resources.

Security Requirements – types and levels of protection necessary for equipment, data, information, applications and facilities to meet laws, Executive Orders, directives, policies, or regulations.

Sensitive Information – "Sensitive information" is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security Number; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system shall be considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

With the exception of certain types of information protected by statute (e.g. Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency.

Spoofing – the interception, alteration, and retransmission of a cipher signal or data in such a way as to mislead the recipient. It is also an attempt to gain access to an information system by posing as an authorized user.

Stand-Alone System- IT resource that is not connected to either a general support system or major application. Stand-Alone systems are often set up to allow an organization to access certain external sites or IT resources in a manner that limits risk to critical enterprise systems. This access is usually designed to be independent of and disconnected from the enterprise network. Examples of Stand-Alone systems include workstations setup to access particular law enforcement databases, contractor network, or when organizational mission requires anonymous access to external systems or networks. If a Stand-Alone system becomes connected to any CBP network, it no longer is a Stand-Alone system and is then subject to CBP security policies and procedures governing all CBP IT assets, including certification and accreditation as appropriate.

Tampering – occurs when an attacker modifies the content of intercepted packets from a wireless network, which results in a loss of data integrity.

Technical Controls – safeguards and countermeasures applied to information systems that are primarily executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat – a potential for harm; an action or event that could cause harm to an IT system.

Trust Zone – A Trust Zone consists of a group of people, information resources, data systems, and/or networks subject to a shared security policy (set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

Type Certification – the certification acceptance of replica information systems based on the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards. This is done in support of the accreditation process to establish the extent to which a particular design and implementation meet a specified set of security requirements.

Virus – a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself. Note that any program that transmits itself as defined above is considered a virus under this definition, whether or not its intent is malicious. Other subsets of viruses include worms and Trojan horses.

Vital Records- Electronic and hardcopy documents, references, records, databases, and IT systems needed to support essential functions under the full spectrum of emergencies. Categories of these types of records may include:

- *Emergency operating records*—emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical Department operations, as well as related policy or procedural records.
- *Legal and financial rights records*—protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as “rights-and-interests” records.

- *Records used to perform national security preparedness functions and activities (E.O. 12656).*

Vulnerability – a flaw or weakness in a system's design, implementation, operation or management that would allow unauthorized use or unauthorized access to the system.

Vulnerability Assessment – formal description and evaluation of the vulnerabilities in an information system.

2.0 Acronyms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Acronym	Meaning
3DES	Triple Data Encryption Standard (usually:
AC	Access Control (800-53 Security Controls)
AC	Assistant Commissioner
ACD	Automatic Call Distribution
ACL	Access Control List
ACS	Automated Commercial System
ADP	Automated Data Processing
AES	Advanced Encryption Standard
APO	Army Post Office
ARP	Address Resolution Protocol
AT	Awareness and Training
ATM	Asynchronous Transfer Mode
ATO	Authorization to Operate
AU	Audit and Accountability (800-53 Security Controls)
BI	Background Investigation
BLSR	Baseline Security Requirements
C&A	Certification and Accreditation
CA	Certification Agent
CA	Certification, Accreditation, and Security Assessments (800-53 Security Controls)
CBP	U.S. Customs and Border Protection
CCB	Change Control Board

Acronym	Meaning
CCEVS	Common Criteria Evaluation and Validation Scheme (NIAP)
CD	Compact Disk
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CFR	Code of Federal Regulation
CGI	Common Gateway Interface
CI	Counter Intelligence
CIA	Confidentiality, Integrity, and Availability
CIFS	Common Internet File Server
CIO	Chief Information Officer
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer at CBP
CM	Configuration Management
CO	Certifying Official
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plans
COTR	Contracting Officer's Technical Representative
COTS	Commercial of the Shelf
CP	Contingency Planning (800-53 Security Controls)
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CPS	Certification Practices Statement
CRC	Cyclic Redundancy Codes
CSIRC	Computer Security Incident Response Center
CSU	Communications Service Units
CTS	Computerized Telephone Systems
CVE	Common Vulnerabilities and Exposures

Acronym	Meaning
DAA	Designated Accrediting Authority at CBP
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration
DHS	Department of Homeland Security
DHS CERT	DHS Computer Emergency Readiness Team
DHS-CFO	Department of Homeland Security Chief Financial Officer
DHS-CIO	Department of Homeland Security Chief Information Officer
DHS-CISO	Department of Homeland Security Chief Information Security Officer
DHS-CPO	Department of Homeland Security Chief Privacy Officer
DHS-SOC	Department of Homeland Security - Security Operations Center
DMZ	De-Militarized Zone
DoD	Department of Defense
DoS	Denial of Service
DR	Disaster Recovery
DSL	Digital Subscriber Line
DSU	Data Service Units
DT&E	Development, Test, and Evaluation
DVD	Digital Video Disk
E.O.	Executive Order
EA	Enterprise Architecture
EACOE	Enterprise Architecture Center of Excellence
EDME	Enterprise Data Management and Engineering Division
ESS	Enterprise Security Services
FAM	Foreign Affairs Manual
FAR	Federal Acquisition Regulation
FEMIA	Federal Financial Management Improvement Act
FIPS	Federal Information Processing Standards (NIST)

Acronym	Meaning
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act of 1982
FOUO	For Official Use Only
FTP	File Transfer Protocol
FY	Fiscal Year
FYHSP	Future Years Homeland Security Program
GSS	General Support System
GAO	General Accounting Office
GIG	Global Information Grid
GSA	General Service Administration
HIDS	Host-based Intrusion Detection Systems
HSAR	Department of Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HTTP	Hyper-Text Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
I&A	Identification and Authentication
I&A	Intelligence and Analysis
IA	Internal Affairs
IA	Identification and Authentication (800-53 Security Controls)
IA	Information Assurance
IA	Internal Affairs
IATO	Interim Authorization to Operate
IAVA	Information Assurance Vulnerability Assessment
ICMP	Internet Control Message Protocol
ICQ	"I Seek You" Tools

Acronym	Meaning
ID	Identification
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IG	Inspector General
IM	Instant Messaging
IMP	Investment Management Process
IMRB	Investment Management Review Board
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPT	Integrated Product Team
IR	Incident Response
IR	Infrared
IRM	Information Resources Management
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISSB	Information System Security Board
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISVA	Information Security Vulnerability Alert
ISVB	Information Security Vulnerability Bulletin
ISVM	Information Security Vulnerability Management
IT	Information Technology
ITGC	IT General Controls
ITMRA	Information Technology Management Reform Act
IXC	Inter-Exchange Carrier
KDP	Key Decision Points
KVL	Key Variable Loader

Acronym	Meaning
LAN	Local Area Network
LBI	Limited Background Investigation
LCM	Life Cycle Management
LE	Law Enforcement
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
LRA	Local Registration Authority
MA	Maintenance (800-53 Security Controls)
MA	Major Application
MAC	Media Access Code
MDF	Main Distribution Frame
MGCP	Media Gateway Control Protocol
MMS	Multimedia Messaging Service
MO	Magneto-Optical
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
NAT	Network Address Translation
NDA	On-Disclosure Agreement
NDC	National Data Center
NFR	Notices of Findings and Recommendations
NFS	Network File Services
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology

Acronym	Meaning
NLT	No Later Than
NMS	Network Management System
NSA	National Security Agency
NSF	Nonstandard Facilities
O&M	Operations and Maintenance
OCISO	Office of Chief Information Security Officer
OIG	Office of the Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
ORR	Office of Regulations and Rulings
OT&E	Operational Test and Evaluation
OTAR	Over-the-Air-Rekeying
P25	Project 25
P2P	Peer-to-Peer
PAA	Principal Accrediting Authority
PAT	Port address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PE	Physical and Environmental Protection (800-53 Security Controls)
PED	Portable Electronic Device
PEDS	Personally Owned Portable Devices
PEN	Privacy Event Notification

Acronym	Meaning
PEP	Policy Enforcement Points
PHIG	Privacy Incident Handling Guidance
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIM	Personal Information Manager
PKI	Public Key Infrastructure
PL	Public Law
PL	Planning (800-53 security controls)
PM	Project Manager
PNS	Protected Network Services
POA&M	Plan Of Action and Milestones
POC	Point of Contact
PS	Personnel Security (800-53 security controls)
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analyses
QoS	Quality of Service
RA	Risk Assessment
RA	Registration Authority
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
ROB	Rules of Behavior
ROM	Read Only Memory
RTM	Requirements Traceability Matrix

Acronym	Meaning
SA	System Administrator
SA	System and Services Acquisition
SAR	Security Assessment Report
SBU	Sensitive-But-Unclassified
SC	System and Communications Protection
SCO	Security Control Officer
SF	Standard Form
SFTP	Secure File Transfer Protocol
SFU	Secure Frame Units
SI	System and Information Integrity
SLC	System Life Cycle
SMB	Server Message Block
SME	Subject Matter Expert
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SORN	Systems of Records Notices
SOW	Statement of Work
SP	Special Publication (NIST)
SSH	Secure Shell
SSI	Sensitive Security Information
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Site Security Officers
SSP	System Security Plan
ST&E	Security Testing and Evaluation
STP	Security and Technology Policy (Branch)

Acronym	Meaning
TA	Technical Advisory
TACACS+	Terminal Access Controller Access Control System+
TAF	Trusted Agent FISMA
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOD	Technology Operations Division
TRC	Technology Review Committee
TRM	Technical Reference Model
TSA	Transportation Security Administration
TT&E	Test, Training, and Exercise
U.S.	United States
U.S.C.	United States Code
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WMO	Wireless Management Office
WORM	Write Once Read Many
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WWW	World-Wide-Web

Acronym	Meaning