NIST Special Publication 800-59

Guideline for Identifying an Information System as a National Security System

William C. Barker

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement. Jr.. Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology, Special Publication 800-59
Natl. Inst. Stand. Technol. Spec. Publ. 800-59, 21 pages (*August 2003*)

GUIDELINE FOR IDENTIFICATION OF INFORMATION SYSTEMS AS NATIONAL SECURITY SYSTEMS

Table of Contents

This page intentionally left blank.

1.0 Introduction

This document provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system. The basis for these guidelines is the Federal Information Security Management Act of 2002 (FISMA, Title III, Public Law 107-347, December 17, 2002), which provides government-wide requirements for information security, superseding the Government Information Security Reform Act and the Computer Security Act.

FISMA both provides a framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides for the maintenance of minimum controls required to protect Federal information and information systems. Federal agencies are responsible for providing information security protection of information collected or maintained by or on behalf of the agency and information systems used or operated by or on behalf of the agency. The head of each Federal agency is also responsible for (1) assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support operations or assets under their control; (2) determining the levels of information security appropriate to protect such information and information systems; (3) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and (4) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

Except for national security systems as defined by FISMA, the Secretary of Commerce is responsible for prescribing standards and guidelines pertaining to Federal information systems on the basis of standards and guidelines developed by NIST. The Committee on National Security Systems (CNSS) along with Federal agencies that operate systems falling within the definition of national security systems provide security standards and guidance for national security systems. In addition to defining the term *national security system* FISMA amended the NIST Act, at 15 U.SC. 278g-3(b)(3), to require NIST to provide guidelines for identifying an information system as a national security system. As stated in the House Committee report, "This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements." Report of the Committee on Government Reform, U. S House of Representatives, Report 107-787, November 14, 2002, p. 85.

The Department of Defense and the Director, Central Intelligence have authority to develop policies, guidelines, and standards for national security systems. The Director, Central Intelligence is responsible for policies relating to systems processing intelligence information. The Committee for National Security Systems, whose executive agent is the National Security Agency, was established to develop operating policies, procedures, guidelines, instructions and standards as necessary to implement provisions of the National Policy for the Security of National Security Telecommunications and

Information Systems (see NSTISSD Number 502). The Director of the Office of Management and Budget (OMB) retains responsibility for oversight of national security system information security policies and practices with respect to:

- Overseeing agency compliance with the requirements of Subchapter III of Chapter 35 of Title 44, United States Code, including through any authorized action under Title 40, United States Code, section 11303, to enforce accountability for compliance with such requirements; and

- Reporting to Congress no later than March 1 of each year on agency compliance with the requirements of Subchapter III of Chapter 35 of Title 44 United States Code, including –

    - A summary of the findings of evaluations required by 44 U.S.C. 3545;
    - An assessment of the development, promulgation, and adoption of, and compliance with, standards developed under 15 USC 278g-3 and promulgated under 40 U.S.C. 11331;
    - Significant deficiencies in agency information security practices;
    - Planned remedial action to address such deficiencies; and
    - A summary of, and OMB views on, the report prepared by NIST under 15 USC 278g-3.

Accordingly, the purpose of these guidelines is not to establish requirements for national security systems, but rather to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President.

2.0 Basis for Identification of National Security Systems

The basis for the identification of 'national security systems' is the definition provided in law (44 U.S.C. 3542(b)(2), which was established by FISMA, Title III, Public Law 107-347, December 17, 2002):

"(2)(A) The term `national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified[1] in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."

Systems not meeting any of these criteria are not national security systems. (Further delineation of the legal definition of the term national security system is found in Appendix A to this guideline.)

As described in the House Committee report, FISMA's national security system definition "encompasses the longstanding statutory treatment of military and intelligence

[1] * See Glossary definition for *classified information*. See also Executive Order 13292 under the authority of which information may be classified.

mission-related systems and classified systems." House Report 107-787, p. 77. It combines the "Warner Amendment" national security system definition, e.g., section 5142 of the Clinger-Cohen Act, at 40 U.S.C. 11103(a), and the treatment of classified systems under section 3 of the Computer Security Act of 1987.

3.0 Method for Identifying National Security Systems

3.1 Determination of Responsibilities

The head of each agency is responsible for designating an agency information security official to determine which, if any, agency systems are national security systems.

Each agency is responsible for identification of all national security systems under its ownership or control. Answering each of the questions stated in the National Security System Identification Checklist, provided as Appendix A to this guideline, is one method for documenting the basis for determination. If the answer to any of the questions is affirmative, the system is designated a national security system. Note that use of the specific form provided in Appendix A is not mandatory. Agencies may develop and use an alternate methodology. It is anticipated that some agencies will require answers to additional questions. However, each of the questions listed on the sample checklist should be answered and recorded.

Ideally, a national security system should be designated as early as possible in its life cycle. The set of certification and accreditation standards, policies, procedures, guidelines, and instructions that apply to each system depend on whether or not the system is a national security system. For systems that are currently in operation, and for which no national security determination has been made, such determination should be accomplished as soon as possible.

Under the provisions of Title 44 United States Code § 3542(b)(2)(A)(i)(V), it is possible that some systems not originally established as national security systems may become national security systems as a result of being designated as critical to the direct fulfillment of military or intelligence missions.[2] If the manager of a military or intelligence mission determines that a system is critical to that mission, and the system has not previously been identified as a *national security system*, the manager responsible for that mission must so identify the system to the responsible entity designated by the head of the *agency* that owns and/or operates the system (see Appendix A, Section A.1.5).

When the manager of a military or intelligence mission determines that a system is no longer critical to that mission, or when the mission is terminated, the manager responsible for that mission must so notify the responsible entity designated by the head of the *agency* that owns and/or operates the system, and the system ceases to be designated a *national security system*. [Note that if a system is designated as a national security system and then removed from that designation (and possibly be moved back at a later time), it may prove very difficult to satisfy the changing security requirements on the system. Therefore, such actions should not be taken casually.]

[2] Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications.

3.2 National Security System Identification Checklist

The National Security System Identification Checklist provided in Appendix A includes six questions. An affirmative answer to one or more of the six questions should result in the system being designated as a national security system. The six questions included in the checklist is only the minimum set of questions on which a national security designation may be based.[3] Individual departments and agencies may choose to include additional questions so long as the decision regarding designation of a system as a national security system is based exclusively on the definition provided in Section 2.0 of this guideline.

3.3 Dispute Resolution

In some cases, a system owner may disagree with a determination by an organization supported by the system regarding whether the system is critical to the direct fulfillment of military or *intelligence* missions. If the *agency* that owns and/or operates a system disputes identification of the system as a *national security system*, either the *agency* or the mission manager may submit the issue to both the CNSS and the appropriate office at the Office of Management and Budget (OMB). OMB will coordinate with other cognizant offices of the Executive Office of the President as required.

If there is a dispute regarding security classification of information processed by a system, the dispute must be submitted to the appropriate internal challenge program[4] for resolution. If the dispute cannot be resolved under the internal challenge program, or if a dispute involves more than one agency, the issue may be submitted to the Information Security Oversight Office (ISOO) for resolution. The ISOO may be contacted at Information Security Oversight Office, National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Room 500, Washington, DC 20408.[5] Any remaining issues may be submitted to the National Security Council.

[3] Note that use of the specific form provided in Appendix A is not mandatory.
[4] Section 1.8(b) of E.O. 13292 [7] requires internal challenge programs for resolution of differences regarding classification of information.
[5] Electronic mail address is isoo@nara.gov.

Appendix A: National Security System Identification Checklist

The National Security System Identification Checklist provided in this Appendix includes six questions designed to determine whether the system meets the definition of a national security system provided in Section 2. An affirmative answer to one or more of the six questions should result in the system being designated as a national security system. The checklist contained in this Appendix is only one alternative for documenting the basis for national security system determination. Note that use of the specific form provided herein is not mandatory. A department or agency may develop and use an alternate checklist or methodology.

A.1 Minimum Question Set

In order for a system to be designated a national security system, one of the following questions must be answered in the affirmative:

- Does the function, operation, or use of the system involve intelligence activities?
- Does the function, operation, or use of the system involve cryptologic activities related to national security?
- Does the function, operation, or use of the system involve command and control of military forces?
- Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?
- Is the system critical to the direct fulfillment of military or intelligence missions?
- Does the system store, process, or communicate classified information?

These questions are included in the checklist found in Section A.3 of this guideline. The following paragraphs provide some explanation and/or conditions applying to each question.

A.1.1 Intelligence Activities

For purposes of this guideline, the term "intelligence activity" means all activities that agencies within the Intelligence community are authorized to conduct pursuant to Executive Order 12333, *United States Intelligence Activities*. As authorized by statute[6], intelligence activities may also include counter drug or counter terrorism intelligence that does not concern foreign countries if the intelligence information was collected or developed by 1) an organization or organizations subordinate to the Director of Central

[6] E.g., Chapter 18 of Title 10, United States Code 124 and Chapter 35 of Title 44 United States Code.

Intelligence or 2) National Foreign Intelligence Programs subordinate to the Secretary of Defense. Box 1 on the checklist should be marked yes if and only if the function, operation, or use of the system involves intelligence activities as defined herein.

A.1.2 Cryptologic Activities

For purposes of completing the National Security System Identification Checklist, "cryptologic activities" include signals intelligence activities, covered under intelligence activities, and the solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems. Box 2 should be marked yes if and only if the function, operation, or use of the system involves *cryptologic* activities as defined herein.

A.1.3 Command and Control of Military Forces

For purposes of this guideline, *command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. *Command and control* functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Box 3 of the National Security System Identification Checklist should be marked yes if and only if the function, operation, or use of the system involve *command and control* of military forces.

A.1.4 Weapons and Weapons Systems

For purposes of this guideline, weapons are defined as being limited to weapons owned by and/or under the control of military forces of the United States and any weapons of mass destruction.[7] A *weapons system* is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. Box 4 of the National Security System Identification Checklist should be marked yes if and only if the system involves equipment that is an integral part of a weapon or *weapons system* as defined herein.

A.1.5 Systems Critical to the Direct Fulfillment of Military or Intelligence Missions

Systems that are critical to the direct fulfillment of military or *intelligence* missions are designated as national security systems unless they are to be used exclusively for routine administrative and business applications. Examples of routine administrative and business systems include those having payroll, finance, logistics, and personnel management applications. Systems having high priority products associated with event-based urgency, such as systems critical to direct mission fulfillment by deployed or contingency military forces, are not routine. Box 5 of the National Security System Identification Checklist should be marked yes if and only if the system is critical to the

[7] The term *weapon*, as used herein, encompasses kinetic weapons, other nuclear/biological/chemical (NBC) weapons and computer network attack (CNA) weapons.

direct fulfillment of military or *intelligence* missions and is not used exclusively for routine administrative and business applications.

A.1.6 Classified Systems

A system is a national security system if it processes, stores, or communicates classified information. Executive orders and Acts of Congress have directed that some specific systems are to be protected at all times by procedures that have been established for information that is to be kept classified[8] in order to protect national defense or foreign policy interests. Authority to assign security classifications to information is delegated in Executive Order 12958 as amended by Executive Order 13292. Any system processing information that is determined to be classified based upon one or more agency classification guides is a classified system. Box 6 of the National Security System Identification Checklist should be marked yes if and only if the system contains or processes classified information.

A.2 Optional Checklist Material

The six questions included in the Appendix A checklist is only the minimum set of questions on which a national security designation may be based. Individual departments and agencies may choose to include additional questions so long as the decision regarding designation of a system as a national security system is based exclusively on the definition provided in Section 2.0 of this guideline. Examples of questions that a department or agency may employ to provide clarification, amplification, and/or justification follow:

- Does this system process, store, or transmit military plans?
- Does this system process, store, or transmit information on weapon systems?
- Does this system process, store, or transmit information regarding military operations?
- Does this system process, store, or transmit information on intelligence activities, sources or methods?
- Does this system involve cryptologic activities related to national security?
- Does this system process, store, or transmit information regarding foreign relations or foreign activities?
- Does this system process, store, or transmit information regarding scientific, technological, or economic matters relating to national security, including defense against transnational terrorism?
- Does this system involve programs for safeguarding nuclear materials or facilities?
- Does this system process, store, or transmit information on weapons of mass destruction?
- Does this system process, store, or transmit information on vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, including defense against transnational terrorism?

[8] See Glossary definition for *classified information*.

- Is the information on this system classified in accordance with one or more of your agency's classification guides?

A.3 Checklist

National Security System Identification Checklist		
System Identification:		
Answer each question in the box provided to the right of the question. Answer yes or no.		
(1) Does the function, operation, or use of the system involve intelligence activities?		(1)
(2) Does the function, operation, or use of the system involve cryptologic activities related to national security?		(2)
(3) Does the function, operation, or use of the system involve military command and control of military forces?		(3)
(4) Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?		(4)
(5) If the use of the system is not routine administrative or business applications, is the system critical to the direct fulfillment of military or intelligence missions?		(5)
(6) Does the system store, process, or communicate classified information?		(6)
If the answer to any of the six questions is "Yes", then the system is a *national security system*.		
Is this system a national security system?		
Organization of Respondent:	Address of Organization: Telephone:_____	
Name of Respondent:	Signature of Respondent:	Date: (dd/mm/yy)

Appendix B: References

[10 USC Ch 18] Title 10, United States Code, Chapter 18 – *Military Support for Civilian Law Enforcement Activities*.

[15 USC 278g-3] Title 15, United States Code, Chapter 7 – *National Institute of Standards and Technology,* Section 278g-3 – Information Systems Standards Program.

[40 USC Subt III] Title 40, United States Code, Subtitle III – *Information Technology Management*, Section 11101 – Definitions, and Section 1103 – Applicability to National Security Systems, Public Law 107-217, 8/21/02 [codified the Clinger-Cohen Act].

[44 USC Ch 35(I)] Title 44, United States Code, Chapter 35 - *Coordination of Federal Information Policy*, Subchapter I - Federal Information Policy, Sec. 3502 - Definitions.

[44 USC Ch 35(III)] Title 44, United States Code, Chapter 35 – *Coordination of Federal Information Policy*, Subchapter III - Information Security, Sec. 3542 - Definitions, Public Law 107-347,12/17/02.

[47 USC Ch 5] Title 47, United States Code, Chapter 5 – *Wire or Radio Communications*, Subchapter I – General Provisions, Sec. 153 - Definitions.

[50 USC Ch 15] Title 50, United States Code, Chapter 15 – *National Security*, Section 401a – Definitions.

[ANSDIT] American National Standard Dictionary of Information Technology (ANSDIT). (Approved April 5, 2002) (Revision and redesignation of ANSI X3.172-1996).

[CNSS 4009] CNSS Instruction No. 4009, National Information Assurance Glossary, Committee for National Security Systems

[Crypto Pub 1-0] *National Cryptologic Doctrine, Cryptology, Cryptologic Publication 1-0*, National Security Agency October 1, 2001.

[EO 12863] *President's Foreign Intelligence Advisory Board*, Executive Order 12863, 9/13/93.

[EO 13292] *Classified National Security Information*, Executive Order 13292, March 25, 2003. [Amends Executive Order 12958]

[EO 12333] *United States Intelligence Activities, Executive Order 12333*, December 8, 1981

[FISMA] *Federal Information Security Management Act of 2002*, Public Law 107-347, Title III, 12/17/02.

[HSA] *Homeland Security Act of 2002*, Public Law 107-296, Title II – Information Analysis and Infrastructure Protection, Subtitle A – Directorate for Information Analysis and Infrastructure Protection: Access to Information, Section 202 – Access to Information, 11/25/02.

[Joint Pub 1-02] *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Rev. 8/14/02.

[T1.523] *Telcom Glossary 2000,* American National Standards Institute, ANS T1.523-2001, 2001

Appendix C: Glossary of Terms

Definitions of terms provided in this glossary have been extracted from public laws, Executive Branch publications and orders, and American National Standards Institute publications.

Agency -
[44 USC 3502 (1)]

The term 'agency' means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include -

(a) the General Accounting Office;
(b) Federal Election Commission;
(c) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or
(d) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.

Availability -
[44 USC 3542 (b)(1)(C)]

As defined in FISMA, the term 'availability' means ensuring timely and reliable access to and use of information.

Authentication -
[CNSS 4009]

Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Classified Information –
[E.O. 13292]

Classified information or classified national security information means information that has been determined pursuant to E. O. 12958 as amended by E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Command and Control –
[Joint Pub 1-02]

'Command and Control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Confidentiality - [44 USC 3542 (b)(1)(B)]
The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Counterintelligence – [50 USC 401a]
The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Cryptography - [ANSDIT]
The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Cryptologic - [Joint Pub 1-02]
The term 'cryptologic' means of or pertaining to cryptology.

Cryptology - [Crypto Pub 1-0]
Originally the field encompassing both cryptography and cryptanalysis. Today, cryptology in the U.S. Government is the collection and/or exploitation of foreign communications and non-communications emitters, known as SIGINT; and solutions, products, and services, to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems, known as IA.

Executive Agency - [41 USC 403]
An executive department specified in 5 U.S.C., Section 101; a military department specified in 5 U.S.C., Section 102; an independent establishment as defined in 5 U.S.C., Section 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.

Federal Information System– [40 USC 101]
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Independent Regulatory Agency – [44 USC 3502 (5)]
The term 'independent regulatory agency' means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal

Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission.

Information - [Joint Pub 1-02]
1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Assurance – [CNSS 4009]
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Resources – [44 USC 3502 (6)]
The term 'information resources' means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security - [44 USC 3542 (b)(1)]
The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information System - [44 USC 3502 (8)]
The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology – [40 USC 11101 (6)]
The term 'information technology', with respect to an executive agency means 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 the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which

(i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity - [44 USC 3542 (b)(1)(A)]
The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Intelligence - [Joint Pub 1-02] [50 USC Ch 15]
The term 'intelligence' means (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

Intelligence Activities – [EO 12333]
The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities.

Intelligence Community – [EO 12333]
The term 'intelligence community' refers to the following agencies or organizations:
(1) The Central Intelligence Agency (CIA);
(2) The National Security Agency (NSA);
(3) The Defense Intelligence Agency (DIA);
(4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(5) The Bureau of Intelligence and Research of the Department of State;
(6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(7) The staff elements of the Director of Central Intelligence.

Non-repudiation - [CNSS 4009]
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Public Information - [44 USC 3502 (12)]
The term 'public information' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.

Telecommunications – [47 USC 5 153]
The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Weapons System - [Joint Pub 1-02]
A 'weapons system' is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.