Draft NISTIR 7298
Revision 3

Glossary of Key Information Security Terms

Celia Paulsen

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

Draft NISTIR 7298
Revision 3

Glossary of Key Information Security Terms

Celia Paulsen

Computer Security Division
Information Technology Laboratory

September 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 7298 Revision 3
11 pages (September 2018)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: ***September 28, 2018*** **through** ***November 30, 2018***

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: secglossary@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. 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 management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This publication describes an online glossary of terms used in National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) publications. This glossary utilizes a database of terms extracted from NIST Federal Information Processing Standards (FIPS), the NIST Special Publication (SP) 800 series, selected NIST Interagency and Internal Reports (NISTIRs), and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009).

Keywords

cybersecurity; definitions; glossary; information assurance; information security; terminology

Supplemental Content

The online glossary described in this publication is publicly available at https://csrc.nist.gov/glossary.

Note to Reviewers

We encourage careful review of the online glossary as well as the methodology described in this publication (e.g. the layout of the database, the content provided in the online application, etc.). Specifically, we request feedback on any areas that may need changes to improve the accuracy and long-term usability of the glossary and the associated database.

Table of Contents

1 Introduction

The National Institute of Standards and Technology (NIST) has created an easily accessible repository of terms and definitions extracted verbatim from NIST Federal Information Processing Standards (FIPS), Special Publications (SPs), and Internal or Interagency Reports (IRs), as well as from the Committee on National Security Systems Instruction 4009 (CNSSI-4009).

This repository ("the Glossary") is intended to help users understand terminology, recognize when and where multiple definitions may exist, and identify a definition that they can use. Over time, use of this Glossary will help standardize terms and definitions used, reducing confusion and the tendency to create unique definitions for different situations.

This publication provides a broad overview of the Glossary's design. It describes the methodology, assumptions, and constraints used in the development of the database and associated online application, available at https://csrc.nist.gov/glossary. Specific implementation details are not provided.

This publication differs significantly from previous versions of NIST IR 7298. Previous versions contained a subset of basic terms that were most frequently used in NIST publications. This method was valuable, but greater demand and frequent updates to NIST's publication suite has necessitated the adoption of a more flexible solution.

2 Methodology

The Glossary contains two main parts: an online application and a database. The database, used as the foundation for the online application, contains terms and definitions extracted verbatim from NIST FIPS, SPs, and IRs, as well as from CNSSI-4009. This database will be updated regularly to accommodate new or updated NIST publications. The database may also be expanded to include withdrawn publications and relevant terms in external or supplemental sources such as applicable laws and regulations. Recommendations for publications to be included in the database can be sent to secglossary@nist.gov. The database does not contain definitions without a source publication. Since draft documents are not stable, the database will not include their terms or definitions.

The online application was developed to allow users to search the database of terms and definitions. It will be updated as necessary to improve functionality and usability.

2.1 Database Structure

The Glossary uses a relational database to store and organize terms, definitions, and their associated sources. A relational database is used to provide a structured, consistent, and durable schema. The database is designed to allow for the following assumptions:

(1) A term may be related to one or more other terms. Terms may be considered identical but differ due to misspellings, alternative spellings, or abbreviations. These can be combined under a single "parent term".
(2) A term-abbreviation, -synonym, or other related pair may be associated with a source.
(3) A term may have one or more definitions.
(4) A definition defines one or more terms.
(5) A term-definition pair is associated with a source.
(6) A source may adapt or copy a term-definition pair from a referenced source.

Figure 1 shows a basic entity-relationship diagram of the database, excluding attributes or relationship types, with numbers corresponding to the above assumptions.

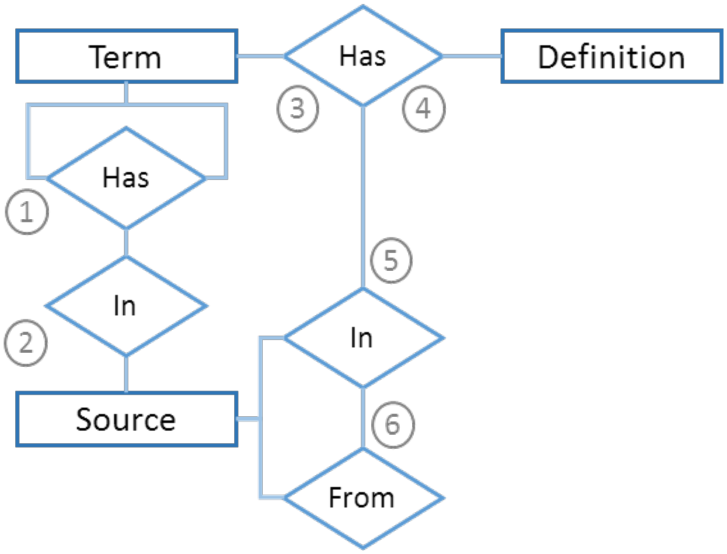

Figure 1: A basic Entity-Relationship diagram for the glossary database

2.2 Data

The glossaries, acronym lists, and equation lists of CNSSI-4009 and NIST FIPS, SPs, and IRs related to cybersecurity, information security or privacy are taken verbatim from their source and entered into the database. If a publication has no glossary, it is quickly scanned for terms explicitly defined within the text of the publication.

Because the Glossary is meant to reflect definitions published by NIST and CNSSI 4009, the relevant information is copied into the database as-is, meaning any errors (e.g., misspellings) in the publications are carried through into the database. The only times the text is altered from the original is when the definition includes a reference (e.g., "as defined in [1]"), in which case the reference is spelled out (e.g., "as defined in NIST SP 800-53"), when possible.

Terms that are referenced in NIST publications using various spellings or abbreviations (e.g., "control" vs. "controls") are identified and linked to a *parent term* (e.g., "control(s)"). These parent terms may or may not be used in NIST publications. They are used in the online application to group like terms together. Besides these parent terms, the database does not currently contain terms or definitions that do not have a source NIST or CNSS publication. On occasion, NIST receives a request to define a term: these requests are forwarded to authors responsible for publishing content related to that term. They may choose to define the term in a publication, in which case it will be included in the glossary database.

The database may have more than one definition for a single term. This occurs for many reasons: definitions can evolve over time, a broad definition may be tailored to a specific subject area, an existing definition may be altered to fit a unique topic, or there could be errors. Because some definitions may have more "weight" or are more broadly recognized than others, definitions are prioritized by assigning each definition's source to one of these ranked categories[1, 2]:

(1) The definition is quoted (i.e., not adapted) from a federal law or regulation.
(2) The definition is quoted from an international, federal, or widely adopted technical standard (e.g., ISO, FIPS, ANSI), a common English or mathematical dictionary, or is an authoritative original technical source (e.g., the Defense Discovery Metadata Specification for the definition of the Defense Discovery Metadata Standard).
(3) The definition is quoted from an Office of Management and Budget (OMB) Policy or Circular, CNSS Policies and Directives, or similar documents.
(4) The definition is from NIST SPs, CNSS Instructions, OMB Memorandum, similar documents, or a specialized dictionary.
(5) The definition is from Government Accountability Office (GAO) Reports, CNSS Advisory Memoranda, Agency-specific standards, regulations, and policies.
(6) The definition is from NIST IRs, white papers, academic or technical papers, or other publications.
(7) The definition is from draft, archived, or superseded publications.

This ranking is not intended to reflect the importance of a publication or definition, but rather is intended as a means to describe the authoritative status of a definition from a general U.S. Federal Government agency point of view. The online application uses these rankings to determine the display order of definitions.

2.3 Web Application

The online application was developed to allow users to search the database of terms and definitions. It is expected that users will typically use the application in order to either (1) gain a better understanding of a term, or (2) find a definition to use. It will be regularly updated to improve functionality and usability based on user feedback.

[1] Definitions that are "adapted" from another source are considered unique and the referenced source is not considered in this ranking. However, if there is no indication that the definition is adapted or altered from the referenced source, then the referenced source is considered. For example, if a NIST IR uses a definition from an international standards body, it will be listed under category 2 unless the NIST IR states that the definition is adapted, in which case it will be listed under category 6.

[2] A source may reference multiple other sources for a definition or may fit multiple categories; in these cases, the highest ranked category is assigned.

The application was designed to be visually similar to other web pages on the NIST Computer Security Resource Center (CSRC) website[3] and attempts to provide as much relevant information as possible to the user. This means that the application may, for example, state that there are no known acronyms for a term (instead of hiding that field). Additionally, there may be multiple definitions for a term that are very similar, yet different. However, this can result in increased complexity as the number of terms and associated definitions grows. It may become necessary to add functionality to the online application to limit searches to only those that are current (i.e. not withdrawn or superceded) or from higher-category sources (e.g., categories 1 and 2 only).

The application is hosted at https://csrc.nist.gov/glossary.

3 Feedback and Updates

The glossary database will be regularly updated as new publications are finalized. Archived publications or publications from other sources (e.g., laws or standards) may be added. Recommendations for publications to be included in the database can be sent to secglossary@nist.gov.

Database entries themselves will rarely be modified. Any change to a NIST document results in a new source—identified by a separate revision number or a new publication date—which would create a new source in the database; thus the change would be treated as a new addition. The old publication and associated definitions will not be removed, but will be marked as superseded or withdrawn, as appropriate. This will enable users to track changes to terms and definitions over time. Two exceptions to this rule are:

- When an error is identified and corrected; and
- The addition of previously unknown information.

Occasionally, it is unclear what version of a document a term originates from (i.e., a referenced source). For these situations, the entry references a source with “unknown” information. This entry may be modified if the exact referenced source later becomes known. The database does not contain definitions without a source publication. Since draft documents are not stable, the database will not include terms/definitions in them.

The application may be updated frequently depending on user feedback. Users are encouraged to provide feedback on the usability of the application or if they identify any bugs in the application. Users are also encouraged to notify NIST of any errors in the glossary database, especially instances where the glossary does not match the term/definition in the associated publication.

[3] https://csrc.nist.gov.

Users may provide feedback on the web application by sending an email to secglossary@nist.gov.