

# Withdrawn Draft

## Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

**Withdrawal Date** July 3, 2019

**Original Release Date** September 28, 2018

## Superseding Document

**Status** Final

**Series/Number** NIST Internal or Interagency Report (NISTIR) 7298 Revision 3

**Title** Glossary of Key Information Security Terms

**Publication Date** July 2019

**DOI** <https://doi.org/10.6028/NIST.IR.7298r3>

**CSRC URL** <https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final>

**Additional Information** CSRC Online Glossary

<https://csrc.nist.gov/glossary>

**Draft NISTIR 7298**  
**Revision 3**

# **Glossary of Key Information Security Terms**

Celia Paulsen

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17

**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*

18  
19  
  
20  
21  
22  
23  
  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40

41  
42  
43  
44  
45  
46  
47  
48

49  
50

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

51  
52  
53  
54

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.

55  
56  
57  
58  
59  
60

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.

61  
62  
63

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>.

64

[11/13/2018: Comment period extended.]

65

**Public comment period: September 28, 2018 through December 21, 2018**

66  
67  
68  
69

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](mailto:secglossary@nist.gov)

70

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

71

72

**Reports on Computer Systems Technology**

73 The Information Technology Laboratory (ITL) at the National Institute of Standards and  
74 Technology (NIST) promotes the U.S. economy and public welfare by providing technical  
75 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test  
76 methods, reference data, proof of concept implementations, and technical analyses to advance the  
77 development and productive use of information technology. ITL's responsibilities include the  
78 development of management, administrative, technical, and physical standards and guidelines for  
79 the cost-effective security and privacy of other than national security-related information in federal  
80 information systems.

81

82

**Abstract**

83 This publication describes an online glossary of terms used in National Institute of Standards and  
84 Technology (NIST) and Committee on National Security Systems (CNSS) publications. This  
85 glossary utilizes a database of terms extracted from NIST Federal Information Processing  
86 Standards (FIPS), the NIST Special Publication (SP) 800 series, selected NIST Interagency and  
87 Internal Reports (NISTIRs), and from the Committee for National Security Systems Instruction  
88 4009 (CNSSI-4009).

89

**Keywords**

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

91

92

93

### **Supplemental Content**

94 The online glossary described in this publication is publicly available at

95 <https://csrc.nist.gov/glossary>.

96

### **Note to Reviewers**

97 We encourage careful review of the online glossary as well as the methodology described in this  
98 publication (e.g. the layout of the database, the content provided in the online application, etc.).

99 Specifically, we request feedback on any areas that may need changes to improve the accuracy  
100 and long-term usability of the glossary and the associated database.

101 **Table of Contents**

102 **1 Introduction ..... 1**

103 **2 Methodology ..... 1**

104 2.1 Database Structure ..... 1

105 2.2 Data ..... 2

106 2.3 Web Application ..... 3

107 **3 Feedback and Updates ..... 4**

108

## 109 **1 Introduction**

110 The National Institute of Standards and Technology (NIST) has created an easily accessible  
111 repository of terms and definitions extracted verbatim from NIST Federal Information  
112 Processing Standards (FIPS), Special Publications (SPs), and Internal or Interagency Reports  
113 (IRs), as well as from the Committee on National Security Systems Instruction 4009 (CNSSI-  
114 4009).

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

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

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

## 127 **2 Methodology**

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

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

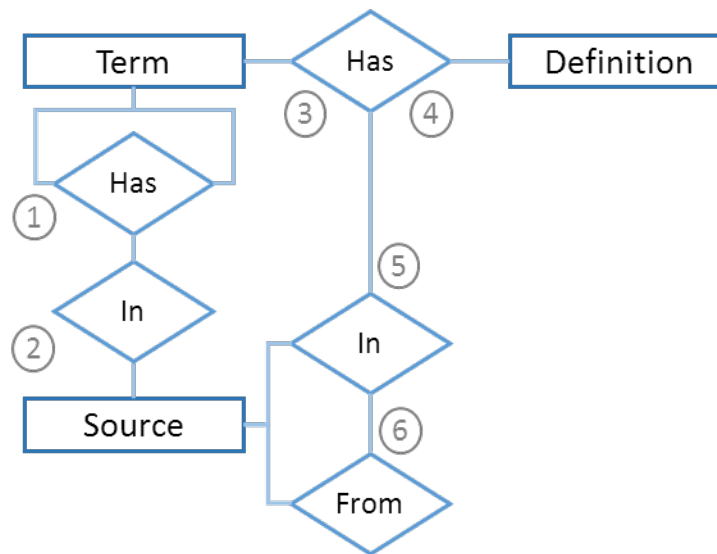
### 139 **2.1 Database Structure**

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



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

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



153

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

## 155 2.2 Data

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

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

165 Terms that are referenced in NIST publications using various spellings or abbreviations (e.g.,  
 166 “control” vs. “controls”) are identified and linked to a *parent term* (e.g., “control(s)”). These  
 167 parent terms may or may not be used in NIST publications. They are used in the online  
 168 application to group like terms together. Besides these parent terms, the database does not

169 currently contain terms or definitions that do not have a source NIST or CNSS publication. On  
170 occasion, NIST receives a request to define a term: these requests are forwarded to authors  
171 responsible for publishing content related to that term. They may choose to define the term in a  
172 publication, in which case it will be included in the glossary database.

173 The database may have more than one definition for a single term. This occurs for many reasons:  
174 definitions can evolve over time, a broad definition may be tailored to a specific subject area, an  
175 existing definition may be altered to fit a unique topic, or there could be errors. Because some  
176 definitions may have more “weight” or are more broadly recognized than others, definitions are  
177 prioritized by assigning each definition’s source to one of these ranked categories<sup>1, 2</sup>:

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

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

## 196 **2.3 Web Application**

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

---

<sup>1</sup> 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.

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

201 The application was designed to be visually similar to other web pages on the NIST Computer  
202 Security Resource Center (CSRC) website<sup>3</sup> and attempts to provide as much relevant  
203 information as possible to the user. This means that the application may, for example, state that  
204 there are no known acronyms for a term (instead of hiding that field). Additionally, there may be  
205 multiple definitions for a term that are very similar, yet different. However, this can result in  
206 increased complexity as the number of terms and associated definitions grows. It may become  
207 necessary to add functionality to the online application to limit searches to only those that are  
208 current (i.e. not withdrawn or superceded) or from higher-category sources (e.g., categories 1 and  
209 2 only).

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

### 211 **3 Feedback and Updates**

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

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

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

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

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

---

<sup>3</sup> <https://csrc.nist.gov>.

234 Users may provide feedback on the web application by sending an email to [secglossary@nist.gov](mailto:secglossary@nist.gov).