NISTIR 7298
Revision 2

Glossary of Key Information Security Terms

Richard Kissel, Editor

http://dx.doi.org/10.6028/NIST.IR.7298r2

This publication is intended to be informative, guiding users to term definitions that exist in various NIST standards and guidelines (along with terms in external publications like CNSSI-4009). This document is out-of-date, and does not reflect additions, deletions, or modifications of term definitions that have occurred since May 2013.

Although this publication is being reviewed and updated, NIST encourages users to review the more up-to-date online glossary, available at https://csrc.nist.gov/glossary.

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

NISTIR 7298
Revision 2

Glossary of Key Information Security Terms

Richard Kissel, Editor
Computer Security Division
Information Technology Laboratory

http://dx.doi.org/10.6028/NIST.IR.7298r2

May 2013

U.S. Department of Commerce
Rebecca Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency or Internal Report 7298r2
222 pages (May 2013)

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

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

The National Institute of Standards and Technology (NIST) has received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners. As a result of these requests, this glossary of common security terms has been extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, NIST Interagency Reports (NISTIRs), and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009). This glossary includes most of the terms in the NIST publications. It also contains nearly all of the terms and definitions from CNSSI-4009. This glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications. For a given term, we do not include all definitions in NIST documents – especially not from the older NIST publications. Since draft documents are not stable, we do not refer to terms/definitions in them.

Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. The NIST publications referenced are the most recent versions of those publications (as of the date of this document).

Keywords

Cyber Security; Definitions; Glossary; Information Assurance; Information Security; Terms

Introduction

We have received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners. As a result of these requests, this glossary of common security terms has been extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, NIST Interagency Reports (NISTIRs), and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009). The glossary includes most of the terms in the NIST publications. It also contains nearly all of the terms and definitions from CNSSI-4009. The glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications. For a given term, we do not include all definitions in NIST documents – especially not from the older NIST publications. Since draft documents are not stable, we do not refer to terms/definitions in them.

Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. A list of the supplemental (non-NIST) sources may be found on pages 221-222. As we are continuously refreshing our publication suite, terms included in the glossary come from our more recent publications. The NIST publications referenced are the most recent versions of those publications (as of the date of this document).

It is our intention to keep the glossary current by providing updates online. New definitions will be added to the glossary as required, and updated versions will be posted on the Computer Security Resource Center (CSRC) Web site at http://csrc.nist.gov/.

The Editor, Richard Kissel, would like to express special thanks to Ms. Tanya Brewer for her outstanding work in the design of the original cover page and in the overall design and organization of the document. Thanks also to all who provided comments during the public review period of this document. The Editor also expresses special thanks to the CNSS Glossary Working Group for encouraging the inclusion of CNSSI-4009 terms and definitions into this glossary.

Comments and suggestions on this publication should be sent to secglossary@nist.gov.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.