1.

Record Nr.	UNINA9910698282203321
Autore	Grance Tim
Titolo	Security Guide for Interconnecting Information Systems: Recommendations of the National Institute of Standards and Technology
Pubbl/distr/stampa	[Place of publication not identified], : DIANE Publishing Company, 2002
Descrizione fisica	1 online resource (iii, 56 pages) : illustrations
Collana	NIST special publication ; ; 800-47. Computer security
Disciplina	005.8
Soggetti	Computer networks - Standards - United States Computer networks - Security measures Computer networks - Standards
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Sommario/riassunto	The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations. The guidelines are consistent with the requirements specified in the Office of Management and Budget (OMB) Circular A-130, Appendix III, for system interconnection and information sharing. A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. The document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection. The document then presents a "life-cycle management" approach for interconnecting IT systems, with an emphasis on security. The four phases of the interconnection life cycle are addressed: 1) Planning the interconnection: the participating organizations perform preliminary activities; examine all relevant technical, security, and administrative issues; and form an agreement governing the management, operation,

and use of the interconnection. 2) Establishing the interconnection: the organizations develop and execute a plan for establishing the interconnection, including implementing or configuring appropriate security controls. 3) Maintaining the interconnection: the organizations actively maintain the interconnection after it is established to ensure that it operates properly and securely. 4) Disconnecting the interconnection: one or both organizations may choose to terminate the interconnection. The termination should be conducted in a planned manner to avoid disrupting the other party's system. In response to an emergency, however, one or both organizations may decide to terminate the interconnection immediately. The document provides recommended steps for completing each phase, emphasizing security measures that should be taken to protect the connected systems and shared data. The document also contains guides and samples for developing an Interconnection Security Agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). The ISA specifies the technical and security requirements of the interconnection, and the MOU/A defines the responsibilities of the participating organizations. Finally, the document contains a guide for developing a System Interconnection Implementation Plan, which defines the process for establishing the interconnection, including scheduling and costs.