1. Record Nr. UNINA9910220113503321

| | |
|---|---|
| Autore | Snyder Don <1962-> |
| Titolo | Improving the cybersecurity of U.S. Air Force military systems throughout their life cycles |
| Pubbl/distr/stampa | [Place of publication not identified] : , : Rand Corporation, , 2015 |
| ISBN | 0-8330-9338-X |
| Collana | Research reports  Improving the cybersecurity of U.S. Air Force military systems throughout their life cycles. |
| Soggetti | Computer networks - Security measures - 21st century - United States<br>Cyberinfrastructure - Evaluation - Security measures - 21st century - United States<br>Computer security - United States<br>Risk assessment - Prevention - United States<br>Cyberterrorism - United States<br>National security<br>Telecommunications<br>Electrical & Computer Engineering<br>Engineering & Applied Sciences |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Bibliographic Level Mode of Issuance: Monograph |
| Nota di contenuto | 1. Cybersecurity Management: Introduction -- What Should Cybersecurity in Acquisition Achieve? -- Managing Cybersecurity Risk -- Challenges for Managing Cybersecurity -- Principles for Managing Cybersecurity -- Principles for Managing Cybersecurity -- Summary -- 2.  Cybersecurity Laws and Policies -- Introduction -- Legislation and Federal Cybersecurity Policy -- Department of Defense Cybersecurity Policy -- Cybersecurity and Air Force Life-Cycle Management -- Conclusion -- 3.  Findings and Recommendations: Findings -- Discussion -- Recommendations -- Closing Remarks. |
| Sommario/riassunto | "There is increasing concern that Air Force systems containing information technology are vulnerable to intelligence exploitation and offensive attack through cyberspace. In this report, the authors analyze how the Air Force acquisition/life-cycle management community can |

improve cybersecurity throughout the life cycle of its military systems. The focus is primarily on the subset of procured systems for which the Air Force has some control over design, architectures, protocols, and interfaces (e.g., weapon systems, platform information technology), as opposed to commercial, off-the-shelf information technology and business systems. The main themes in the authors' findings are that cybersecurity laws and policies were created to manage commercial, off-the-shelf information technology and business systems and do not adequately address the challenges of securing military systems. Nor do they adequately capture the impact to operational missions. Cybersecurity is mainly added on to systems, not designed in. The authors recommend 12 steps that the Air Force can take to improve the cybersecurity of its military systems throughout their life cycles"--Provided by publisher.