



# **21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON**

*U.S. Government, Department of Defense, U.S. Military, U.S. Air Force*

[Download now](#)

[Click here](#) if your download doesn't start automatically

# **21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON**

*U.S. Government, Department of Defense, U.S. Military, U.S. Air Force*

**21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON** U.S. Government, Department of Defense, U.S. Military, U.S. Air Force

The Department of Defense maintains a comprehensive cyber incident handling program. This program ensures an integrated capability to continually improve the Department of Defense's ability to rapidly identify and respond to cyber incidents that adversely affect DoD information networks and information systems (ISs). It does so in a way that is consistent, repeatable, quality driven, measurable, and understood across DoD organizations. This provides requirements and methodology for establishing, operating, and maintaining a robust DoD cyber incident handling capability for routine response to events and incidents within the Department of Defense.

CYBER INCIDENT HANDLING PROGRAM \* Introduction \* Roles and Responsibilities \* Computer Network Defense Overview \* Computer Network Defense Services \* Computer Network Defense Sustainment Functions \* ENCLOSURE B \* CYBER INCIDENT HANDLING METHODOLOGY \* Introduction \* Cyber Incident Handling Process and Life Cycle \* Submit Initial Report \* Preliminary Response Actions \* Cyber Incident Analysis \* Response and Recovery \* Post-Incident Analysis \* First Responder Guidelines \* APPENDIX A TO ENCLOSURE B \* CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIZATION \* Introduction \* Categories \* Comparison of DoD and Department of Homeland Security (DHS) \* Categories \* ENCLOSURE C \* CYBER INCIDENT REPORTING \* Introduction \* Reporting Structures \* Operational Reporting Practices \* Reporting Vehicles \* Reporting Timelines \* Reporting Formats \* Reporting Considerations \* Exercise Reporting \* APPENDIX A TO ENCLOSURE C \* REPORTING TIMELINES \* Introduction \* Reporting Timelines \* APPENDIX B TO ENCLOSURE C \* GENERAL CYBER INCIDENT REPORT FORMAT \* General Cyber Incident Report Format \* Initial Impact Assessment Matrix \* APPENDIX C TO ENCLOSURE C \* CYBER INCIDENT REPORTING DIAGRAMS \* High-Level Overview of Reporting \* Cyber Event Detected by Installation \* Cyber Event Detected Within Combatant Command \* Cyber Event Detected by External CND Group \* Cyber Event Detected by Computer Network Defense Services Provider \* ENCLOSURE D \* CYBER INCIDENT ANALYSIS \* Introduction \* Cyber Incident Analysis Framework \* Computer Forensics Analysis \* System Analysis \* Malware Analysis \* Network Analysis \* Analysis and Correlation of Cyber Event and Cyber Incident Data \* Legal Issues \* APPENDIX A TO ENCLOSURE D \* DELIVERY VECTORS \* Introduction \* Delivery Vector Categories \* APPENDIX B TO ENCLOSURE D \* SYSTEM WEAKNESSES \* Introduction \* Determining Information System Weaknesses \* APPENDIX C TO ENCLOSURE D \* IMPACT ASSESSMENT MATRIX \* Impact Assessment \* Levels of Impact \* Determining Technical and Operational Impact \* Cyber Incident Impact Table \* Cyber Incident and Event Potential Impact \* ENCLOSURE E \* CYBER INCIDENT RESPONSE \* Introduction \* Types of Responses \* Developing and Implementing Courses of Action \* Recovering Without Performing Technical Analysis \* Containment Eradication Recovery Post-Incident Activity \* ENCLOSURE F \* COLLABORATION WITH OTHER STRATEGIC COMMUNITIES \* Introduction \* Operational Cooperation with LE/CI \* International Coordination \* Intelligence Community \* Cyber Unified

Coordination Group \* APPENDIX A TO ENCLOSURE F \* COORDINATION AND DECONFLICTION \*  
Introduction \* Types of Operations \* APPENDIX B TO ENCLOSURE F \* INTELLIGENCE SUPPORT  
TO CYBER INCIDENT REPORTING \* Introduction \* Joint Incident Management System (JIMS) \*  
Intelligence Reporting Procedures \* Product Dissemination \* Writing For Release \* USCYBERCOM  
"Smart Book" \* ENCLOSURE G \* COMPUTER NETWORK DEFENSE INCIDENT HANDLING TOOLS  
\* Joint Incident Management System (JIMS) \* Joint Malware Catalog (JMC) \* Cyber Intelligence Analysis  
Tools \* DoD Protected Traffic List \* DoD Enterprise Incident Sets \* DoD Information Network Deception  
Projects \* Cyber Condition (CYBERCON)

 [Download 21st Century U.S. Military Documents: Cyber Incide ...pdf](#)

 [Read Online 21st Century U.S. Military Documents: Cyber Inci ...pdf](#)

## **Download and Read Free Online 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON U.S. Government, Department of Defense, U.S. Military, U.S. Air Force**

---

### **From reader reviews:**

#### **Dale Perez:**

Why don't make it to become your habit? Right now, try to prepare your time to do the important behave, like looking for your favorite publication and reading a e-book. Beside you can solve your long lasting problem; you can add your knowledge by the guide entitled 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON. Try to make book 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON as your buddy. It means that it can for being your friend when you feel alone and beside that course make you smarter than ever before. Yeah, it is very fortunated to suit your needs. The book makes you more confidence because you can know everything by the book. So , let me make new experience in addition to knowledge with this book.

#### **Cheryl Fenske:**

This 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON book is not really ordinary book, you have after that it the world is in your hands. The benefit you obtain by reading this book is actually information inside this e-book incredible fresh, you will get information which is getting deeper you actually read a lot of information you will get. This 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON without we comprehend teach the one who reading it become critical in imagining and analyzing. Don't end up being worry 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON can bring whenever you are and not make your case space or bookshelves' turn out to be full because you can have it in your lovely laptop even mobile phone. This 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON having excellent arrangement in word as well as layout, so you will not experience uninterested in reading.

#### **Lionel Huggins:**

The book 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON will bring that you the new experience of reading any book. The author style to clarify the idea is very unique. If you try to find new book to learn, this book very ideal to you. The book 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON is much recommended to you you just read. You can also get the e-book from the official web site, so you can quicker to read the book.

**Pearl Miller:**

Are you kind of hectic person, only have 10 or maybe 15 minute in your morning to upgrading your mind talent or thinking skill actually analytical thinking? Then you are receiving problem with the book compared to can satisfy your short time to read it because all of this time you only find publication that need more time to be learn. 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON can be your answer given it can be read by an individual who have those short time problems.

**Download and Read Online 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON U.S. Government, Department of Defense, U.S. Military, U.S. Air Force #31IYLRC5POZ**

## **Read 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force for online ebook**

21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force books to read online.

## **Online 21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force ebook PDF download**

**21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force Doc**

**21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force Mobipocket**

**21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON by U.S. Government, Department of Defense, U.S. Military, U.S. Air Force EPub**