Dod Joint Security Implementation Guide June 2015

Cyber Warfare: A Documentary and Reference GuideMonth in review Defense logistics better strategic planning can help ensure DOD's successful implementation of passive radio frequency identification : report to congressional committees.Intelligence, Surveillance, and ReconnaissanceOperation Iraqi Freedom: DoD Should Apply Lessons Learned Concerning the Need for Security over Conventional Munitions Storage Sites to Future Operations PlanningDSCA HandbookDefense Space ActivitiesHearing on Sharing of VA/DOD Electronic Health InformationVision Working Group Report and ScenariosManuals Combined: DoD Security Engineering Facilities Planning; Design Guide For Physical Security Of Buildings; Antiterrorism Standards For Buildings And Specifications For Active Vehicle BarriersJoint and National Intelligence Support to Military OperationsHomeland DefenseThe U.S. Army War College Guide to National Security Issues: Theory of war and strategyMaritime SecurityVA and DoD Health Care: First Federal Health Care Center Established, but Implementation Concerns Need to be AddressedCertified Enterprise Architect All-in-One Exam GuideJoint Staff Officers GuideJoint Logistics Commanders' guide for the management of joint service programsPerformance Management: DOD Is Terminating the National Security Personnel System, but Needs a Strategic Plan to Guide Its Design of a

New SystemProliferationFORCEnet Implementation StrategyDoD Information Security ProgramAir Force Officer's GuideDefense acquisitions the Global Information Grid and challenges facing its implementation : report to Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives.National Security Strategy of the United StatesCombating terrorism actions needed to guide services' antiterrorism efforts at installations.Personnel Security ClearancesIntelligence, Surveillance, and Reconnaissance: DoD needs a Strategic, Risk-Based Approach to Enhance Its Maritime Domain AwarenessStrategic Theory for the 21st Century: The Little Book on Big StrategyDoD Supply Chain Management Implementation GuideGovernment Reports Annual IndexCivilian Personnel Management: Dodi 1400.25FISMA Compliance HandbookProceedings of the Annual Seminar/Symposium, Project Management InstituteDefense LogisticsDod-Joint Special Access Program (Sap) Implementation Guide (Jsig)Linux Pocket GuideThe McGraw-Hill Homeland Security Handbook : The Definitive Guide for Law Enforcement, EMT, and All Other Security ProfessionalsDoD Digital Modernization StrategyNATL INDUSTRIAL SECURITY PROGR

Cyber Warfare: A Documentary and Reference Guide

This effective study guide offers comprehensive coverage of topics comprising the enterprise architecture body of knowledge. The book provides detailed coverage and lays out actionable methodologies and best practices to create and maintain successful EA models, artifacts and building blocks. It helps prepare readers to take any of the various EA certification exams and academic courses in enterprise architecture. This highly effective self-study guide offers comprehensive coverage of all topics in the enterprise architecture body of knowledge. Written by a team of experienced academics, practitioners, and professionals, the book takes a holistic look at the practice of enterprise architecture. You will get actionable methodologies and best practices and learn how to develop, deploy, and maintain successful enterprise architecture models, artifacts, and building blocks. Designed to help you prepare for certification, the Certified Enterprise Architect All-in-One Exam Guide also serves as an essential on-the-job reference. Coverage includes:•Enterprise architecture foundation concepts•Planning the enterprise architecture•Enterprise architecture development, governance, and maintenance•Defense frameworks•Viewpoints and views•The Zachman Framework•The Open Group Architecture Framework (TOGAF)•The Common Approach to Federal Enterprise Architecture•FEAF2•Comparison of frameworks•Case Study integrated throughout the text•And much more

Month in review

Defense logistics better strategic planning can help ensure DOD's successful implementation of passive radio frequency identification : report to congressional committees.

The DoD¿s intelligence, surveillance, and reconnaissance (ISR) capabilities -- such as satellites and unmanned aircraft systems -- are crucial to military operations, and demand for ISR capabilities has increased. Congress directed DoD to fully integrate its ISR capabilities, also known as the ISR enterprise, as it works to meet current and future ISR needs. This report: (1) describes the challenges that DoD faces in integrating its ISR enterprise; (2) assesses DoD¿s mgmt. approach for improving integration of its future ISR investments; and (3) evaluates the extent to which DoD has implemented key activities to ensure proposed new ISR capabilities fill gaps, are not duplicative, and use a joint approach to meeting war-fighters¿ needs. Illustrations.

Intelligence, Surveillance, and Reconnaissance

Personnel security clearances are used to verify that national security information -- which in some cases could cause exceptionally grave damage to national security if disclosed -- is entrusted only to those who have proven reliability and loyalty to the nation. In response to long-standing problems with timeliness

and backlogs, Congress mandated clearance reforms as part of the Intelligence Reform and Terrorism Prevention Act of 2004. This report reviews the extent to which reform efforts: (1) align with key practices for organizational transformations; and (2) address identified factors for reforming the personnel security clearance process. Includes recommendations. Tables.

Operation Iraqi Freedom: DoD Should Apply Lessons Learned Concerning the Need for Security over Conventional Munitions Storage Sites to Future Operations Planning

DSCA Handbook

Defense Space Activities

"The DoD Supply Chain Management Implementation Guide is a tool to assist logistics personnel who are responsible for implementing supply chain management. This Guide presents the key supply chain principles and implementation strategies compiled into a structured and workable approach for achieving progress toward fully incorporating supply chain management into the DoD logistics process. This document is Intended to serve as a roadmap for individuals and organizations seeking day-to-day direction for implementing supply chain management

in a DoD environment."--DTIC abstracts.

Hearing on Sharing of VA/DOD Electronic Health Information

Vision Working Group Report and Scenarios

The global threat landscape is constantly evolving and remaining competitive and modernizing our digital environment for great power competition is imperative for the Department of Defense. We must act now to secure our future.This Digital Modernization Strategy is the cornerstone for advancing our digital environment to afford the Joint Force a competitive advantage in the modern battlespace.Our approach is simple. We will increase technological capabilities across the Department and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena. We will achieve this through four strategic initiatives: innovation for advantage, optimization, resilient cybersecurity, and cultivation of talent.The Digital Modernization Strategy provides a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control and communications and cybersecurity.This approach will enable increased lethality for the Joint warfighter, empower new partnerships that will drive mission success, and implement new reforms enacted to improve capabilities across the information

enterprise.The strategy also highlights two important elements that will create an enduring and outcome driven strategy. First, it articulates an enterprise view of the future where more common foundational technology is delivered across the DoD Components. Secondly, the strategy calls for a Management System that drives outcomes through a metric driven approach, tied to new DoD CIO authorities granted by Congress for both technology budgets and standards.As we modernize our digital environment across the Department, we must recognize now more than ever the importance of collaboration with our industry and academic partners. I expect the senior leaders of our Department, the Services, and the Joint Warfighting community to take the intent and guidance in this strategy and drive implementation to achieve results in support of our mission to Defend the Nation.

Manuals Combined: DoD Security Engineering Facilities Planning; Design Guide For Physical Security Of Buildings; Antiterrorism Standards For Buildings And Specifications For Active Vehicle Barriers

U.S. Northern Command (NORTHCOM) exercises to test preparedness to perform its homeland defense and civil support missions. This report assesses the extent to which NORTHCOM is: (1) consistent with Department of Defense (DoD) training and exercise requirements; (2) involving interagency partners and states in its exercises; (3) using lessons learned and

corrective actions to improve preparedness; and (4) integrating its exercises with the National Exercise Program (NEP). To do this, the auditor reviewed NORTHCOM and NEP guidance and post-exercise documentation, assessed NORTHCOM compliance, and compared DoD and NEP exercise requirements. Charts and tables.

Joint and National Intelligence Support to Military Operations

Somali pirates have attacked 640 ships and taken over 3,150 hostages since 2007. A few U.S.-flagged vessels have been affected -- most recently the SV Quest, a private yacht on which four Amer. were killed in Feb. 2011. The growing frequency and severity of attacks renew the urgency to address the piracy threat. As Somalia is unable to repress piracy, the NSC developed the Countering Piracy off the Horn of Africa: Action Plan in Dec. 2008 to prevent, disrupt, and prosecute piracy in collaboration with international and industry partners. In Sept. 2010, a report evaluated the extent to which U.S. agencies: (1) have implemented the plan, and the challenges they face; and (2) have collaborated with partners. This is a print on demand report.

Homeland Defense

Offers access to the 1997 "Proliferation: Threat and Response" report from the United States Department of Defense. Details nuclear, biological, chemical, and other weapon proliferation in Asian, Middle Eastern,

and former Soviet areas. Provides access to related news releases and a press briefing transcript. Links to related sites.

The U.S. Army War College Guide to National Security Issues: Theory of war and strategy

This two-in one resource includes the Tactical Commanders and Staff Toolkit plus the Liaison Officer Toolkit. Defense Support of Civil Authorities (DSCA)) enables tactical level Commanders and their Staffs to properly plan and execute assigned DSCA missions for all hazard operations, excluding Chemical, Biological, Radiological, Nuclear, high yield Explosives (CBRNE) or acts of terrorism. Applies to all United States military forces, including Department of Defense (DOD) components (Active and Reserve forces and National Guard when in Federal Status). This hand-on resource also may be useful information for local and state first responders. Chapter 1 contains background information relative to Defense Support of Civil Authorities (DSCA) including legal, doctinal, and policy issues. Chapter 2 provides an overview of the incident management processes including National Response Framework (NRF), National Incident Management Systems (NIMS), and Incident Command System (ICS) as well as Department of Homeland Security (DHS). Chapter 3 discuses the civilian and military responses to natural disaster. Chapter 4 provides a brief overview of Joint Operation Planning Process and mission analyis. Chapter 5 covers Defense Support of Civilian

Authorities (DSCA) planning factors for response to all hazard events. Chapter 6 is review of safety and operational composite risk management processes Chapters 7-11 contain Concepts of Operation (CONOPS) and details five natrual hazards/disasters and the pertinent planning factors for each within the scope of DSCA.

Maritime Security

VA and DoD Health Care: First Federal Health Care Center Established, but Implementation Concerns Need to be Addressed

Certified Enterprise Architect All-in-One Exam Guide

Joint Staff Officers Guide

Joint Logistics Commanders' guide for the management of joint service programs

DODI 1400.25 Civilian Personnel Management - This book is Volume 1 of 4. This information was updated 8/22/2018. Buy the paperback from Amazon, get Kindle eBook FREE using Amazon MATCHBOOK. go to

www.usgovpub.com to learn how.Volume 1. Chapter 100 to 805 Volume 2. Chapter 810 to 1406 Volume 3. Chapter 1407 to 1800 Volume 4. Chapter 2001 to 3007 (DCIPS) The purpose of the overall Instruction is to establish and implement policy, establish uniform DoD-wide procedures, provide guidelines and model programs, delegate authority, and assign responsibilities regarding civilian personnel management within the Department of Defense. Why buy a book you can download for free? We print this book so you don't have to. First you gotta find a good clean (legible) copy and make sure it's the latest version (not always easy). Some documents found on the web are missing some pages or the image quality is so poor, they are difficult to read. We look over each document carefully and replace poor quality images by going back to the original source document. We proof each document to make sure it's all there - including all changes. If you find a good copy, you could print it using a network printer you share with 100 other people (typically its either out of paper or toner). If it's just a 10-page document, no problem, but if it's 250-pages, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. It's much more cost-effective to just order the latest version from Amazon.com This book includes original commentary which is copyright material. Note that government documents are in the public domain. We print these large documents as a service so you don't have to. The books are compact, tightly-bound, full-size (8 1⁄2 by 11 inches), with large text and glossy covers. 4th Watch Publishing Co. is a SDVOSB. www.usgovpub.com

Performance Management: DOD Is Terminating the National Security Personnel System, but Needs a Strategic Plan to Guide Its Design of a New System

This edition of the U. S. Army War College Guide to National Security Policy and Strategy continues to reflect the structure and approach of the core national security strategy and policy curriculum at the War College. The fourth edition is published in two volumes that correspond roughly to the Department of National Security and Strategy's core courses: "Theory of War and Strategy" and "National Security Policy and Strategy." Like previous editions, this one is largely an expansion of its predecessor rather than a major rewriting. About a quarter of the chapters are new, and several others have undergone significant rewrites or updates. However, approximately half of the book remains unchanged. Although this is not primarily a textbook, it does reflect both the method and manner we use to teach strategy formulation to America's future senior leaders. The book is not a comprehensive or exhaustive treatment of either strategic theory or the policymaking process. Both volumes are organized to proceed from the general to the specific. Thus the first volume opens with general thoughts on the nature and theory of war and strategy, proceeds to look at the complex aspect of power, and concludes with specific theoretical issues. Similarly, the second volume begins by examining the policy/strategy process, moves to a look at the strategic environment, and concludes with some specific issues. This edition adds several short case

studies that can be used to illustrate the primary material in the volume.

Proliferation

The Dept. of Defense¿s (DoD) operational dependence on space has placed new and increasing demands on current space systems to meet commanders¿ needs. DoD¿s Operationally Responsive Space (ORS) concept is designed to more rapidly satisfy commanders¿ needs for information and intelligence during ongoing operations. Given the potential for ORS to change how DoD acquires and fields space capabilities to support the warfighter, this report discusses to what extent DoD: (1) is developing ORS to support warfighter requirements; and (2) has a plan that integrates ORS into existing DoD and intelligence community processes and architecture. Includes recommendations. Charts and tables.

FORCEnet Implementation Strategy

DoD Information Security Program

DoDi 5200.01 Incorporating Change 1, Effective May 1, 2018 This book contains all 4 volumes of DoD Instruction (DoDI) 5200.01 current to 1 May 2018 and updates policy and responsibilities for collateral, special access program, SCI, and controlled unclassified information (CUI). The DoD Information Security Program is intended to harmonize and align processes to the maximum extent possible to

promote information sharing, facilitate use of scarce resources, and simplify its management and implementation. SCI will be safeguarded in accordance with policies and procedures established by the DNI. Why buy a book you can download for free? We print this book so you don't have to. First you gotta find a good clean (legible) copy and make sure it's the latest version (not always easy). Some documents found on the web are missing some pages or the image quality is so poor, they are difficult to read. We look over each document carefully and replace poor quality images by going back to the original source document. We proof each document to make sure it's all there - including all changes. If you find a good copy, you could print it using a network printer you share with 100 other people (typically its either out of paper or toner). If it's just a 10-page document, no problem, but if it's 250-pages, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. It's much more cost-effective to just order the latest version from Amazon.com This book includes original commentary which is copyright material. Note that government documents are in the public domain. We print these large documents as a service so you don't have to. The books are compact, tightly-bound, full-size (8 1⁄2 by 11 inches), with large text and glossy covers. If you like the service we provide, please leave positive review on Amazon.com. Without positive feedback from the community, we may discontinue the service and y'all can go back to printing these books manually yourselves. For more titles, visit www.usgovpub.com

Air Force Officer's Guide

"The McGraw-Hill Homeland Security Handbook provides government officials, corporate risk and security executives, first responders, university students, and all homeland security and emergency preparedness professionals with a definitive overview of our nation's critical homeland security issues. This all-in-one reference features analyses, insights, and practical recommendations from frontline security experts."--BOOK JACKET.

Defense acquisitions the Global Information Grid and challenges facing its implementation : report to Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives.

National Security Strategy of the United States

The Project on National Security Reform submitted its 2-year study of the national security system, Forging a New Shield, to the President, President-elect, and Congress on November 26, 2008. Before the Project finalized the report's recommendations, its Vision Working Group tested the findings against a diverse set of scenarios to determine if the recommendations were robust and effective. This volume documents

the scenario-testing process used by the Vision Working Group and includes the actual pre-reform and post-reform scenarios and details many other scenario techniques used in the overall study. Results revealed that each of the five major findings improved the performance of the current national security system, but, on the whole, the findings concluded that the national security system was at risk of failure and needed serious reform. The work of the Vision Working Group has led to the formulation of an additional recommendation: The country must establish a mechanism to infuse greater foresight into the Executive Branch, and in particular the national security system. This proposed mechanism, named the Center for Strategic Analysis and Assessment, would exist and operate within the Executive Office of the President. This volume details the proposed architecture and operation of the Center.

Combating terrorism actions needed to guide services' antiterrorism efforts at installations.

This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. FISMA Compliance Handbook Second Edition explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The evolution of Certification and Accreditation is discussed. This book walks the reader through the entire FISMA compliance process and includes guidance on how to manage a FISMA compliance project from start to finish. The book has

chapters for all FISMA compliance deliverables and includes information on how to conduct a FISMA compliant security assessment. Various topics discussed in this book include the NIST Risk Management Framework, how to characterize the sensitivity level of your system, contingency plan, system security plan development, security awareness training, privacy impact assessments, security assessments and more. Readers will learn how to obtain an Authority to Operate for an information system and what actions to take in regards to vulnerabilities and audit findings. FISMA Compliance Handbook Second Edition, also includes all-new coverage of federal cloud computing compliance from author Laura Taylor, the federal government's technical lead for FedRAMP, the government program used to assess and authorize cloud products and services. Includes new information on cloud computing compliance from Laura Taylor, the federal government's technical lead for FedRAMP Includes coverage for both corporate and government IT managers Learn how to prepare for, perform, and document FISMA compliance projects This book is used by various colleges and universities in information security and MBA curriculums

Personnel Security Clearances

Intelligence, Surveillance, and Reconnaissance: DoD needs a Strategic, Risk-Based Approach to Enhance Its Maritime Domain Awareness

Strategic Theory for the 21st Century: The Little Book on Big Strategy

FORCEnet is currently defined as the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed, combat force that is scalable across all levels of conflict from seabed to space and sea to land. Although this definition views FORCEnet as the operational construct and the architectural framework for the entire transformed Navy, some have viewed FORCEnet merely as an information network and the associated FORCEnet architecture merely as an information systems architecture. FORCEnet Implementation Strategy provides advice regarding both the adequacy of this definition and the actions required to implement FORCEnet.

DoD Supply Chain Management Implementation Guide

Air Force officers of all ranks, from cadets to generals, both active duty and reserves, will find this revised edition essential reading for a successful career.

Government Reports Annual Index

1-100. Purpose. This Manual: a. Is issued in accordance with the National Industrial Security

Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations (CFR). b. Incorporates and cancels DoD 5220.22-M, Supplement 1 (reference (ab)).

Civilian Personnel Management: Dodi 1400.25

Establishes guidance on the provision of joint and national intelligence products, services, and support to military operations. Describes the org. of joint intelligence forces and the national Intelligence Community, intelligence responsibilities, command relationships, and national intelligence support mechanisms. Provides info. regarding the fundamentals of intelligence operations and the intelligence process, discusses how intelligence supports joint and multinational planning, and

describes intelligence dissemination via the global info. grid. Provides military guidance for the exercise of authority by combatant commanders and other joint force commanders. Illustrations. A print on demand edition of a hard to find report.

FISMA Compliance Handbook

Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable

work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare. Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade

Proceedings of the Annual Seminar/Symposium, Project Management Institute

Defense Logistics

O'Reilly's Pocket Guides have earned a reputation as inexpensive, comprehensive, and compact guides that have the stuff but not the fluff. Every page of Linux Pocket Guide lives up to this billing. It clearly explains how to get up to speed quickly on day-to-day Linux use. Once you're up and running, Linux Pocket Guide provides an easy-to-use reference that you can keep by your keyboard for those times when you want a fast, useful answer, not hours in the man pages. Linux Pocket Guide is organized the way you use Linux: by function, not just alphabetically. It's not the

'bible of Linux; it's a practical and concise guide to the options and commands you need most. It starts with general concepts like files and directories, the shell, and X windows, and then presents detailed overviews of the most essential commands, with clear examples. You'll learn each command's purpose, usage, options, location on disk, and even the RPM package that installed it. The Linux Pocket Guide is tailored to Fedora Linux--the latest spin-off of Red Hat Linux--but most of the information applies to any Linux system. Throw in a host of valuable power user tips and a friendly and accessible style, and you'll quickly find this practical, to-the-point book a small but mighty resource for Linux users.

Dod-Joint Special Access Program (Sap) Implementation Guide (Jsig)

The National Defense Authorizaiton Act (NDAA) for FY 2010 authorized the Departments of Veterans Affairs (VA) and the DoD to establish a 5-year demonstration proejct to integrate VA and DoD medical care into a first-of-its-kind Federal Health Care Center (FHCC) in North Chicago, Illinois. Expectations for the FHCC are outlined in a Executive Agreement signed by VA and DoD in April 2010. This report evaluates various aspects of the FHCC integration. It examines: (1) what progress VA and DoD have made implementing the Executive Agreement to establish and operate the FHCC; and (2) what plan, if any, VA and DoD have to assess FHCC provision of care and operations. Charts and tables. This is a print on demand report.

Linux Pocket Guide

Over 1,600 total pages . Application and Use: Commanders, security and antiterrorism personnel, planners, and other members of project planning teams will use this to establish project specific design criteria for DoD facilities, estimate the costs for implementing those criteria, and evaluating both the design criteria and the options for implementing it. The design criteria and costs will be incorporated into project programming documents.

The McGraw-Hill Homeland Security Handbook : The Definitive Guide for Law Enforcement, EMT, and All Other Security Professionals

Special Access Programs represent some of the Department's most sensitive information and must be protected accordingly. We can no longer rely on physical isolation as a primary risk mitigation strategy. Threats and risks often outpace our ability to implant robust, multi-disciplinary countermeasures. Cost and timelines to develop threats to our data almost always pale to the cost and time to implement countermeasures. Given the rapid increase in cybersecurity threats and prioritization from the SECDEF, the senior cybersecurity professionals responsible for authorizing information systems to process SAP have identified three security controls which offer mitigations so significant they can no longer be tailored. Beginning in this revision of the JSIG, we are introducing controls that are not

tailorable. Historically, the ability to tailor controls has been delegated to the field but senior leadership is no longer willing to accept the risk of high volume data loss. Recognizing there may be extreme situations in which it is not feasible to implement these controls in their entirety, the authority to tailor or modify these controls is delegated to the component SAP senior authorizing official. This waiver authority cannot be further delegated. The establishment of a senior authorizing official for each DoD component will elevate the status of cybersecurity functions so they more effectively influence department-wide strategy, policy, and investments. The Risk Management Framework (RMF) is a framework designed to be tailored to meet organizational needs while providing adequate risk management of data and information systems. Transformation to the RMF is a daunting task and we appreciate all the effort to date within the Department and Industry. We applaud all the hard work of the Joint SAP Cybersecurity Working Group (JSCS WG) and the spectacular leadership of the individuals who created this joint "coalition of the willing."

DoD Digital Modernization Strategy

Maritime security threats to the U.S. are broad, incl. the naval forces of potential adversary nations, terrorism, and piracy. The attacks on the USS Cole in 2000, in Mumbai in 2008, and on the Maersk Alabama in 2009 highlight these threats. DoD considers maritime domain awareness -- identifying threats and providing commanders with sufficient awareness to

make timely decisions -- a means for facilitating effective action in the maritime domain and critical to its homeland defense mission. This report examines the extent to which DoD has developed a strategy to manage its maritime domain awareness efforts and uses a risk-based approach. It is a public version of a previous, sensitive report. Charts and tables. This is a print on demand report.

NATL INDUSTRIAL SECURITY PROGR

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION