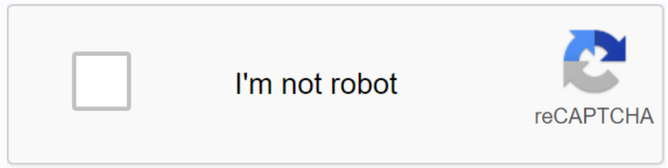

Continue

Joint security implementation guide jsig

CSCI is looking for a well-qualified and self-confident Information Systems Security Manager (ISSM) to support a Department of Defense (DoD) client based in Arlington, La. Applicants must have experience in the construction and maintenance of infrastructures that meet and adhere to the control set out in the DoD Intelligence System (DoDIIS) – Joint Security Implementation Guide (DJSIG) and the DoD Implementation Manual (JSIG). The above mentioned Directives need to implement and support the risk management framework, which is a successful experience in implementing and supporting the risk management framework. All applicants require experience to deploy and support the Information Protection Agency (DISA) Secure Technical Implementation Guides (STIG) for Red Hat Linux and Microsoft Windows Server operating systems. Day-to-day activities include: it serves as an MSM for multiple systems and ensures that system processes are followed by all staff, including privileged users. Create and maintain System Security Plans (SSP), Traceability Security Control Matrix (SCTM), Action plan and Important Events (POA&M) and any other RMF documentation required for supported systems. View and evaluate RMF packages from external organizations to provide information and recommendations for official (AO) resolution. Perform an SCAP Compatibility Checker (SCC) scan to make sure the configurations comply with the latest DISA STIG. Perform an Nessus Security scan to ensure that all known vulnerabilities are mitigated or documented within a System Action plan and Important Events (POA&M). Interface with external persons with regard to the maintenance of authorisation of existing infrastructures. Performs systematic audits on multiple platforms and implements processes and technologies that help highlight anomalies that can be evaluated to ensure confidentiality, integrity and availability is not compromised. Maintain a strong security position for all supported infrastructures. The candidate requires the following: Excellent communication skills. Strong writing skills to create and view RMF documentation. Strong technical skills with Linux and Windows operating systems to go along with a deep understanding of the RMF process. Ability to work effectively with others, which helps to promote and promote a positive working environment. Experience: Requires a minimum of 5 years of experience working as an Information System Security Officer (ISSO) or the information issm supporting DCID, ICD 705, JDODIIS, JAFAN, DJSIG and/or JSIG. RMF implementation and maintenance experience is required. Education: BA/BS or AA/AS in information technology, cybersecurity discipline related to them. Training/certification: DoD 8570 Compliance. IAM Level III Certification (GSLC, CISM and/or CISSP) desired. U.S. Citizenship: Yes Minimum Permit: Applicants are required to have at least TOP SECRET SECRET permission Part of the eligibility criteria for information based on a single scope study (SSBI) completed in the last 5 years. The selected candidates must be prepared to submit to the initial and random polygraph of counterintelligence data. This exciting career opportunity offers a competitive compensation package, comprehensive benefits and career opportunities. Example: Dental Hygienist Ministry of Defence (DOD). Joint Special Access Program Implementation Guide (SAP) (JSIG). April 11, 2016 Note: This version of JSIG is based on NIST SP 800-53, Rev 4, and CNSSI 1253, March 2014. 1 Introduction and roles STR. Preface. The RMF is a framework designed to meet organisational needs while ensuring adequate data risk management and information systems. Transformation into RMF is a daunting task and we appreciate all the efforts that have so far been within the department and industry. We welcome all the hard work of SAP's Joint Cybersecurity Working Group (JSCS WG) and the spectacular leadership of the individuals who created this JOINT Coalition of The Willing. DEDICATED access programs represent some of the department's most sensitive information and must be adequately protected. Chapter 1 Introduction and roles STR. MINISTRY OF DEFENSE (DOD) JOINT SPECIAL ACCESS PROGRAM (SAP) IMPLEMENTATION GUIDE (JSIG) April 11, 2016 Tags: Programs, Manual, Chapter, Implementation, Special, Access, Special Access Program, Implementation Guide 1 MINISTRY OF DEFENSE (DOD). Joint Special Access Program Implementation Guide (SAP) (JSIG). April 11, 2016 Note: This version of JSIG is based on NIST SP 800-53, Rev 4, and CNSSI 1253, March 2014. 1 Introduction and roles STR. Preface. The RMF is a framework designed to meet organisational needs while ensuring adequate data risk management and information systems. Transformation into RMF is a daunting task and we appreciate all the efforts that have so far been within the department and industry. We welcome all the hard work of SAP's Joint Cybersecurity Working Group (JSCS WG) and the spectacular leadership of the individuals who created this JOINT Coalition of The Willing. SPECIAL access programs represent some of the most sensitive information of the Department and must be protected accordingly.2 We can no longer rely on physical isolation as a basic risk reduction strategy. Threats and risks often outpaced our ability to implant healthy, multidisciplinary counteraction. The costs and deadlines for developing threats to our data are almost always pale to the cost and time of countermeasures. Given the rapid increase in cybersecurity and prioritisation by SECDEF, the senior cybersecurity professionals responsible for authorising information systems for processing have established three security checks which offer such significant safeguards that they can no longer be adapted. At the beginning of this JSIG revision, we introduce controls that are not adapted. Historically, the ability to adjust control has been delegated to the field, but senior leadership is no longer inclined to accept the risk of high volume data loss.3 High volume data recognition can have extreme situations where it is not possible to apply these checks in their entirety, the adjustment or modification body of these controls is delegated to the SAP senior authoritarian component. That exemption authority may not be further delegated. Creating a high official title for each doD component will enhance the status of cybersecurity functions so that they more effectively influence strategy, policy and investment across the DEPARTMENT. Change Summary: Create SAP Component Employees for Higher Authoring o Each doD component responsible for enabling SAP information systems determines in writing SAP Senior Authorization Officer for the component. The current sap authorisation chief officer is the non-pergolable control waiver authority. This authority cannot be delegated.4 A waiver of these checks will be sent to the DoD. sap cio within 30 days of approval. Create non-standard controls o See AC-6(1), Least Privilege | Enabling access to security features ultimate system protection must not be tailored. o See SA-22, Unsupported system components added to the baseline and required to be deployed on all SAP systems. o See SC-28, Resting Data Encryption Protection applies to all SAP systems. This whole document shall enter into force immediately. The government's policy is that all classified information must be adequately guaranteed to ensure the confidentiality, integrity and availability of that information. This document provides standardized security policies and procedures for use in the management of all networks, systems and components under the scope of the DEPARTMENT OF DEFENSE Special Access Program (DOD) and DoD Service /Agency SAPCOs.5 This guide applies to the DoD SAP Community and all networks, information systems, weapons systems and applications for which cogniant SAP. Authorization of official (AO) has responsibility for management or supervision, regardless of physical location. 1 Introduction and roles STR. Responsibilities The SAP Joint Cybersecurity Working Group (JSCS WG) is appropriate to provide guidance on the deployment of cybersecurity to DoD SAP. WP JSCS provides organizations within the DoD SAP Community with a forum to address all aspects of cybersecurity. JSCS's functions and activities for the WP related to the include: Promoting community coordination within the framework of the evaluating and enabling SAP information systems and related areas (documentation, tools, evaluation methods, processes) to ensure consistency in methodologies, approaches, templates, and organization-defined values within DoD SAP within DoD SAP to develop, maintain and periodically update RMF policies and procedures, so as to include, where appropriate, SSIG, security control layering, RMF training, templates, and other supporting documents Encourage, review and update training and awareness objectives, materials and availability for all service partners, agency and industry cybersecurity, emphasizing the threat of inside information, community best practices and RMF.6 Additional information on roles and responsibilities related to the Risk Management Framework , may be in the Effective Date section This document enters into force immediately and organisations should start tracking changes from revision 3 to Revision 4 (new security control of check 4, amended and deleted) in the POA&M information system, with a focus on the three indible controls referred to above. The components may also provide additional transition guidance. This document must be reissued, cancelled or certified within 5 years of its publication in order to be considered relevant. David B. Bill Kenneth R. Bowen Brigadier General, Chief Information Officer of the USAF, Special Access Program Headquarters of the Office doD SPECIAL Access, Chapter 1-Introduction and Rollie PAGE 1-3. Content Content .. 4. 1 INTRODUCTION AND 11.7 INTRODUCTION .. 11. PURPOSE AND APPLICABILITY .. 12. RECIPROCITY .. 12. CHANGES IN 13. ROLES AND RESPONSIBILITIES. 14. Head of the Agency/Component.... 14. Risk Executive Director (function) .. 14. Chief Information Officer (CIO). 15. Chief Information Security Officer (CISO) .. 15. Authorisation of an official (AO) .. 16. Delegated Official Authorisation (DAO) .. 17. Security Control Assessor (SCA) .. 17. Common Control Provider (CCP). 18. Program Security Officer (PPA). 18. Owner of the information/Stewart. 18. Mission/Business Owner (MBO) .. 18. Owner of an information system (ISO) .. 19. Security Information System (ISSE) engineer. 20. Information System Security Manager (ISSM) .. 20. Information System Security Officer (ISSO) .. 21. Privileged users .. 22. General users .. 22. ORGANIZATION OF DOCUMENTS AND USE .. 22. 2 RISK MANAGEMENT FRAMEWORK .. 24. INTRODUCTION TO RMF.8 24. PRINCIPLES OF THE FFM. 25. Risk management within the organisation.. 25. System Development Cycle (SDLC). 26. Information system 28. RMF SIXTH-STEP PROCESS .. 30. RMF Step 1, .. 30. RMF step 2, select .. 33. Step 3 RMF, implementation (development/construction). 35. RMF step 4, Assessment (test). 35. RMF step 5, order (deployment/operation) .. 36. RMF step 6, monitor .. 38. 3 POLICY AND PROCEDURES. 41. FAMILY: Access CONTROL .. 43. AC-1 ACCESS CONTROL POLICY AND PROCEDURES.. 43. AC-2 AC-2 Management.. 43. AC-3 Access Enforcement .. 48. AC-4 APPLICATION OF FLOW INFORMATION .. 51. AK-5 DIVISION OF OBLIGATIONS .. 58. AC-6 LESS PRIVILEGES .. 59. AC-7 FAILED LOGIN ATTEMPTS .. 61. NOTIFICATION OF USE OF THE AC-8 SYSTEM .. 62. AC-9 PREVIOUS LOGIN (ACCESS) NOTIFICATION .. 63. SIMULTANEOUS SESSION OF AC-10 63. AC-11 SESSION LOCK .. 64. Chapter 1 Introduction and Rollie STR. AC-13 Access control and control with 65. AC-14 ENABLED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION.. 65. AC-15 AUTOMATED MARKING.. 66. AC-16 SECURITY 66. AC-17 REMOTE ACCESS .. 69. WIRELESS ACCESS AC-18 .. 70. AC-19 access control for mobile devices .. 71. AC-20 USE OF EXTERNAL INFORMATION SYSTEMS .. 73. AC-21 INFORMATION SHARING .. AC-22 IS PUBLICLY AVAILABLE 76. AC-23 DATA RETRIEVAL PROTECTION.. 77. AC-24 ACCESS CONTROL SOLUTIONS .. 77. AC-25 DATA MONITOR .. 78. FAMILY: AWARENESS AND 79. C-1 SECURITY AND TRAINING AWARENESS-RAISING POLICIES AND PROCEDURES. 79. SECURITY AWARENESS-RAISING TRAINING.. 79. ROLL-3 SECURITY TRAINING.. 80. C-4 SECURITY TRAINING FILE .. 83. LEVEL 5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS .. 83. FAMILY: AUDIT AND ACCOUNTABILITY.. 84. AU-1 AUDIT AND POLICY AND REPORTING PROCEDURES.10 84. AU-2 AUDIT EVENTS .. 85. CONTENT OF AU-3 AUDIT RECORDS. 87. AU-4 STORAGE AUDIT CAPACITY.. 88. AU-5 RESPONSE TO ERRORS IN AUDIT PROCESSING.. 89. AUDIT, ANALYSIS AND REPORTING BY AU-6.. 90. REDUCING THE AU-7 AUDIT AND GENERATING REPORTS .. 92. WE-8 TIME STAMPS .. 93. AU-9 PROTECTION OF AUDIT INFORMATION.. 93. NON-REPREDICTABLE 10TH NON-DEPREVALENT. 95. AUDIT OF AU-11 DOCUMENT 96. AU-12 AUDIT PRODUCTION .. 97. AU-13 MONITORING FOR DISCLOSURE OF INFORMATION .. 97. AU-14 SESSION AUDIT .. 98. ALTERNATIVE AUDIT OF AU-15 CAPABILITY. 98. AU-16 INTERORGANISATION 99. FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION .. 100. CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES.. 100. CA-2 SECURITY ASSESSMENTS .. 100. CA-3SYSTEM CONNECTIONS .. 104. CA-4 SECURITY CERTIFICATE .. 105. CA-5 ACTION PLAN AND 105. CA-6 SECURITY CLEARANCE. Related Search Search Search Search: CATEGORIZATION AND CONTROL,1253, 1253, 1253, Austro-Security System, Revised Statute Title 33 – Property, CHAPTER, Programmable Logic Controllers, Content Title 46 PROFESSIONAL and Chapter 2 Accounting Review: Income Reports, Chapter 2 Accounting: Income Reports and Chapter SIX RISE OF THE LODGE, Global Report on Violence and Health, INDUSTRIAL SECURITY REPORT,