Kerryl Cacho

CONTACT

32.7464809,-117.1987256,17

E-mail: cyber@cyb3r.33mail.com

Website: http://www.kerrylcacho.com

Phone: 1-702-582-5147

PROFESSIONAL SUMMARY

Over 18 years in positions of increasing responsibility within the U.S. Armed Forces, Designed, implemented, and managed numerous programs; conducted seminars and briefing sessions for senior level management. Developed, initiated, and evaluated new procedures, policies, and internal controls; assessed and resolved complex operational problems and holds a Top Secret SCI Eligible-National agency check with Local agency check clearance. The goal is to manage Information Technology (specifically information security and contingency planning) projects in direct support of the Government Information Security Reform Act (GISRA), Federal Information Security Management Act (FISMA), and National Security Strategy.

CORE COMPETENCIES

- Develop security policies, procedures, technical reports, point papers, information technology project planning, intrusion detections analysis reports, contingency plans, disaster recovery, and information systems risk analysis reports to ensure defense against unauthorized access to systems, networks, and data.
- Knowledge of DCID 6/3, DoD IIS/NIST guidelines, Department of Defense (DoD) Information Systems for certification and accreditation (C&A) (DIACAP)/DOD Information Assurance Risk Management Framework (DIARMF), C&A activities (e.g., Certification Testing and Evaluation (CT&E), Security Testing and Evaluation (ST&E)), knowledge of Lean Six Sigma (LSS), Continuous Process Improvement (CPI) principles, and Information Technology Information Library fundamental principles.

WORK EXPERIENCE

SPAWAR HQ 8.2.0 — June 2012 - Present

IT Specialist 2210 (DP-03/GS-13)

- Assigned as the Deputy Project Manager (DPM) to various SPAWAR projects as well as Government liaison to numerous other projects, responsible to ensure a resolutions of technical problems are consistent with the program’s objectives, cost, and performance criteria. Also provided guidance on priority Information Assurance (IA) requirements affecting acquisition programs.
- Maintained standards and procedures to ensure execution of Security strategies; Including enforcement of security regulations, investigations, incident response and continuity of operations for physical security, cyber security, and communication security for SPAWAR Headquarters. Also provided interpretation of policies promulgated by Presidential Directives, Congress, National Institute of Standards (NIST) and other agencies.

- Align SPAWAR's business requirements with IT, while using SPAWAR's current corporate intellectual data on DOD and Navy Global/Regional systems and policies, to ensure compliance of those assets.
- Maintained the development of SPAWAR Information Resource Management (IRM) milestone projects (e.g. metrics reports) for management to ensure proper budgeting to meet enterprise-wide business needs.
- Ensure that information security management processes are integrated with agency strategic and operational planning purposes. Implemented policies and procedures governing the protection of Sensitive Compartmented Information (SCI) facilities, operations, information and material for SPAWAR Headquarters.
- Applied expert knowledge to a wide range of IT practices to advise on alternative approaches for complex application system and to resolve critical problems related to database management systems within SPAWAR HQ.
- Integrate a broad range of disparate technologies into a common denominator of overall functionality to support SPAWAR HQ enterprise business processes.
- Establish policy and procedures for conducting s upporting Defense Security Service (DSS) Computer Network Defense (CND) incidents and Cyber Security Inspection efforts for Sponsored Echelon II Cleared Defense Circuits (CDC).
- Establish policy and procedures for conducting relationships with stakeholders to support the success of IT programs by facilitating the gathering and collection of user account records data used in Inspector General (IG) investigations, criminal investigations, etc. Interface with SPAWAR Network Security Manager, Command IA Managers (IAM) and Network Security staff at SSC-LANT and SSC-PAC about IA matters.
- Analyze end-to-end processes of functions, products, and/or services (e.g. Information Management (IM), Information Technology (IT), IA) in order to achieve enterprise efficiencies by reducing, restructuring, and/or eliminating those that do not contribute to the optimization of resources.
- Established and authored formal correspondences and/or briefing materials (e.g. policies, memorandums for the record, e- mails, executive summaries, brief sheets, PowerPoint slides, etc.) providing information to achieve signature approval and/or authorization for release.

Joint Special Operations Command — June 2015 - June 2016

Cyber Mission Support Integrator (1825)

- Oversee standards and procedures for JSOC to ensure execution of Security strategies; Including enforcement of security regulations, investigations, incident response and continuity of operations for physical security, cyber security, and communication security.
- Supervised workforce planning, resource management and auditing to ensure, physical security, EKMS, and network program compliance as well as operational readiness for Special Forces operators.
- Supported J6 Cybersecurity Branch Chief by initiating personnel actions, interviewing candidates and making recommendations for selection of employees for vacant positions.
- Developed and supervised innovative e-Business and knowledge management solution for JSOC J6 Cybersecurity Branch as well as implementing new e-Business concepts, practices, and technologies.
- Providing technical advice and support to senior level executives by collecting monthly report input from all organizational elements to prepare briefing reports to higher headquarters for JSOC.
- Established and authored Information Assurance (IA) policies (e.g. Federal, Department of Defense (DoD), Joint Information Technology (IT)/IA directives, instructions, Computer/Communications Tasking Orders (CTOs), Warning Orders (WARNORDs), Fragmentation Orders (FRAGOs)) to develop and implement operational performance metrics to ensure delivery of products and services to provide guidance for implementation to JSOC and SOCOM CIO.
- Directed and overseen the installation of system accreditations that provided immediate processing in the event of system failure on JDI, JIANT, and SOCRATES networks at JSOC.

SPAWAR HQ 8.2.4 — August 2011 - June 2012

IT Specialist 2210 (DS-03/GS-12)

- Maintained relationships with stakeholders to support the success of IT programs by facilitating the gathering and collection of user account records data used in Inspector General (IG) investigations, criminal investigations, etc. Interface with SPAWAR Network Security Manager, Command IA Managers (IAM) and Network Security staff at

SSC-LANT and SSC-PAC about IA matters.

- Interpret Information Assurance (IA) policies (e.g. Federal, Department of Defense (DoD), Department of Navy (DoN), Navy Information Technology (IT)/IA directives, instructions, Computer/Communications Tasking Orders (CTOs), Warning Orders (WARNORDs), Fragmentation Orders (FRAGOs)) to develop and implement operational performance metrics to ensure delivery of products and services to provide guidance for implementation to CIO.
- Analyze end-to-end processes of functions, products, and/or services (e.g. Information Management (IM), Information Technology (IT), IA) in order to achieve enterprise efficiencies by reducing, restructuring, and/or eliminating those that do not contribute to the optimization of resources.
- Align SPAWAR's business requirements with IT, while using SPAWAR's current corporate intellectual data on DOD and Navy Global/Regional systems and policies, to ensure compliance of those assets.
- Supported SPAWAR HQ by initiating personnel actions, interviewing candidates and making recommendations for the selection of employees for vacant positions to senior leadership.
- Ensure that information security management processes are integrated with agency strategic and operational planning purposes. Implemented policies and procedures governing the protection of Sensitive Compartmented Information (SCI) facilities, operations, information and material for SPAWAR Headquarters.

QUALIFICATIONS

- DoD Directive 8570.1 Complaint (IAM Level II):GAIC Security Leadership (GSLC)
- Network+
- Server+
- Security+
- Certified Ethical Hacker (CEH)
- Information Assurance Methodology (IAM)
- Information Security Analysis (ISA)
- Information Assurance Policy Management (IAPM)
- Information Systems Security Manager Course
- Intermediate Level Navy Validator I0437
- CNSS certificate 4012 (Senior System Managers)
- CNSS certificate 4015 (System Certifiers)
- Security Fundamentals Professional Certification
- DOD Security Specialist
- Defense Acquisition Workforce Improvement Act (DAWIA) Level II

U.S. MILITARY QUALIFICATIONS

- GA1: IP Basic Qualification
- GA2: IP Intermediate Qualification
- GA7: (IA)
- GC0: Information Dominance Warfare Officer (IDWO) Qualified
- JOM: Operational Level Command and Control Maritime
- 2650: KM OFFICER
- 9519: Information Management Officer
- 3000: Resource Management and Analysis - General

EDUCATION

Masters of Business Administration (MBA)
June 2005 - June 2007

Salem International University

Defense Acquisition Workforce Level II
Jan 2011 - July 2016

Defense Acquisition University

Bachelors of Science in Information Technology
June 2003 - June 2005

University of Phoenix

AWARD

- SPAWAR EXEMPLARY ACHIEVEMENT AWARD 2013
- SPAWAR LIGHTNING BOLT AWARD FOR CTO-13 TASKER IMPLEMENTATION

SECURITY CLEARANCE

Top Secret SCI Eligible-National agency check with Local agency check

REFERENCES

References available upon request.