IT Specialist (PLCYPLN) GG-2210-13 (Step 10) IT Specialist (PLCYPLN) GG-2210-13 (Step 10) Senior Cyber/CNO Analyst - UNITED STATES ARMY Woodbridge, VA Joint Cyber Capabilities and Requirements / Digital Media Forensics - Cyber Security Forensics Examiner / Senior Cyber / CNO Analyst / Cyber Security System Architect / Information Systems Officer / Project Manager and Veteran Military Officer an active Top-Secret Security Clearance Sensitive Compartmentalized Information with Department of Defense Counterintelligence Polygraph offering 30 years of proven Civilian and Military Leadership experience in communications and information systems management at the global enterprise level. Directed planning and operation of communications and network systems support US civilian and military global operations and maintained accountability of $2M+ of classified communications systems. Successfully managed secured and non-secured US Government computer networks of Cyber Workforce users and implemented multiple Cyber Network Defense and Information Security training programs. Recipient of multiple awards and promotions for outstanding performance and professionalism in the United States Army. Career supported by US Army Project Management Certification, a Bachelor of Arts in Business Management and a Master of Arts in Information Technology Management. C|EH/Security+ CE/C|NDA CNE/CNO/MPS/OCO Project Management ICD 503/DCID 6/3 /FISMA/NIST/CNSS POA&M/STIG /COOP RMF/DIACAP/eMASS JWICS/CITRIX/NSAnet IA/Cyber Security/ Analyst KM/SharePoint 2010 SDLC / IT Strategic Planning Authorized to work in the US for any employer Work Experience IT Specialist (PLCYPLN) GG-2210-13 (Step 10) Joint Forces Headquarters Department of Defense Information Networks (JFHQ-DoDIN) - Fort Meade, MD July 2019 to Present Performs as member of the Joint Cyber Capabilities and Requirements Group (JC2RG) the Initial Operational Capability under the Joint Forces Headquarters Department of Defense Information Networks (JFHQ-DoDIN). Mastery of IT security theories and concepts, practices, and emerging issues in addition to project management methods. Applies experimental theories and new developments to information security problems not susceptible to treatment by accepted methods. Broad knowledge of and skill in applying methods for evaluating, implementing, and disseminating IT security tools and procedures enough to coordinate activities designed to

ensure, protect, and restore IT systems, services, and capabilities. Mastery of IT security certification and accreditation requirements to monitor and evaluate systems' compliance with IT security requirements. Knowledge of network operations and protocols to provide advice and guidance in implementing IT security policies and procedures. Knowledge and skill to perform as a technical authority in Information Operations (IO) analysis of large, complex, cross-functional information systems. Extensive practical and theoretical knowledge of IO technical principles, functions, and processes of information management planning and implementation, concepts, trends, and methods, software applications, and information management principles is required. Knowledge of organizational mission, procedures, and goals; Joint Forces Headquarters - Commands (JFHQ-Cs), and other government agencies ADP Security, information procedures, and Privacy Act regulations. Knowledge of operating systems (interactive and batch, personal computer, and minicomputer), capability and applicability of high-level and user-friendly language systems; organizational programming environments; software product lines; hardware capabilities and limitations; and file design. Knowledge of microcomputer operations, configurations, and interfaces to mainframe computers and minicomputers. Knowledge of software tools to support the information automated office environment. Broad knowledge in telecommunications and Local Area Networks (LAN). Knowledge of the latest developments in database design, methodology, data organization structures, structural relationships, processing techniques, data modeling, access methods, data dictionaries/directories, data element naming conventions and standards, automated data and activity modeling tools and methods, and information architecture, to guide the management of the IO applications. Knowledge of information management approaches and techniques to access advanced information technologies, publicized latest developments in technology, and identify possible areas of research to ensure technological advancements can meet IO management needs. Knowledge is required of management processes, organizational design and structure, managerial decision-making, and planning and control of IO operations. Broad knowledge is required in the following functional areas: Personnel. Manpower, Logistics, Finance (Management Information Systems), and Intelligence Production and Dissemination Systems. Analysis and planning

techniques are required to prepare and integrate analyses, organize conflicting requirements, and synthesize data relevant to the data planning process to predict impacts to existing IO plans and systems, to recognize developments potentially applicable to information automated systems, and to generate useful recommendations and plans. Administrative policies and precedents are applicable but are stated only in very general terms. Guidelines for performing the work are scarce or of limited use. The employee uses initiative and resourcefulness in deviating from traditional methods or researching trends and patterns to develop new methods, criteria, or proposed new policies. The work involves ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools. The incumbent identifies issues and resolves criteria/problems that primarily concern IO supported system implementation projects. Incumbent performs the function of a subject matter expert, decision maker, policy generator, and technical advisor for IO system integration, architectural development, and life cycle within a wide spectrum of ADP/Telecommunications Management activities. Makes authoritative decisions and serves as focal point and team leader for providing expert assistance in technical matters, directional guidance on policies and issues to Army and other information operations activities. The work involves analyzing IO situations where technological advances and data/information efficiencies can be implemented, especially for the end-user. Defines IO problems and conditions, formulates projects, and establishes specifications and guidelines. Decisions and commitments often involve large expenditures of resources and have a strong impact on important programs. The employee works independently with JFHQ-Cs, and other national level agencies to facilitate and manage IO technological advances of automated information systems. The results of these activities impact upon the IO operations of JFHQ-Cs, and other national level agencies. The employee sets the overall objectives and resources available. The employee, in consultation, develop the deadlines and projects. The employee is responsible for planning and carrying out the assignment, resolving most of the conflicts that arise, and interpreting policy in terms of established objectives. The employee is kept informed of progress and any controversial matters. Finished work

and methods are reviewed for accuracy and effectiveness and for compliance with complex instructions and guidelines. Digital Media Forensics - Cyber Security Forensics Examiner (Contractor) ManTech International Corporation - Fort Belvoir, VA April 2019 to July 2019 Performed all phases of the forensic examination of digital media, including on-site and off-site evidence acquisition/seizures, forensic analysis, and reporting, ensuring chain of custody is maintained and that applicable rules of evidence are adhered to. Leads efforts for performing post-mortem analysis of the magnetic media, optical media, and volatile data (memory images) collected from compromised systems. Provided testimony related to forensic/malware examinations. Reversed engineering malware, using Dynamic and Static analysis. Support CND tool custom signature and correlation rules creation to enhance enterprise protections based on indicators discovered during the forensics analysis process. Identifies trends in incidents and malware and recommends enterprise protection measures based on incident trends. Researches new attacks and exploits. Writes and publishes cyber incident forensic/malware reports detailing findings and mitigation/remediation recommendations. Develops and documents malware and forensic analysis guidance, processes, and procedures. Contributes to the completion of milestones associated with specific projects. Provides solutions to a variety of complex technical problems. Plans and conducts assignments, generally involving the larger and more important projects or more than one project. Cyber Operations Technologist (Contractor) Booz Allen Hamilton - Quantico, VA March 2019 to April 2019 DEFENSE INTELLIGENCE AGENCY (DIA), OCI4 SAP: Monitors, analyzes, and detects Cyber events and incidents within information systems and networks. Consult on integrated, dynamic Cyber defense and leverage Cybersecurity solutions to administer Cybersecurity operational services, including intrusion detection and prevention, situational awareness of network intrusions, security events and data spillage, and incident response actions. Participate in testing, deploying, and administering the infrastructure hardware and software which are required to effectively manage the organization's Cybersecurity operational services. Senior Cyber/CNO Analyst UNITED STATES ARMY - Washington, DC May 2018 to February 2019 Contractor) Provide subject matter expertise as principal Army cyberspace advisor interfacing across OSD, Joint

Staff, and Army community in support of all aspects of cyberspace operations, to include: DOD Information Network Operations (DODIN Ops), Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). Provide research, analysis and recommendations on cyber-related areas including intelligence support to cyber operations, Defensive Cyber Operations, creating effects in cyberspace, Offensive Cyberspace Operations, DOD Information Network Operations (DODIN Ops), Cyber Situational Awareness, universal IT architecture. Prepare briefings, information/decision papers, policy documents, staffing packages, letters, Execution Orders (EXORDS), memorandums and official multimedia correspondence related to Army cyber concepts, doctrine, and policy. Review and evaluate Army, DOD, Joint and other Services cyber plans and policies to provide analysis and recommendations on integrating Cyberspace Operations throughout the Army and with Information Operations. Know and understand the Command and Control and Organizational Force Structure of the Army and the procedures for completing Army and Joint staff actions. Provide subject matter expertise on Army cyberspace offensive and defensive capabilities and DODIN operations acquisition processes. Review cyberspace operational needs documents and assist in the development of cost-benefit analysis for cyberspace capabilities; manage cyberspace acquisition issues through the Governance Council and Army Cyberspace Council to include the management of Op Ts as required. Perform cost-benefit analysis to determine cyber courses of action. Provide analysis and coordinate with cyber activities and to provide input to Army positions on Cyber training, ranges and platforms, persistent training environment acquisition and sustainment. IT Specialist UNITED STATES ARMY - Fort Belvoir, VA January 2017 to May 2018 InfoSec) GS-13 Senior IT Specialist U.S. Army Cyber Command (ARCYBER) located at Fort Belvoir, Virginia. Serves and performs the duties as the ARCYBER G33 Offensive Current Cyber Operations (OCO) Specialist. Assists the Operations Chief in the day-to-day operations within the 24 X 7 Army Cyber Operations and Integration Center (NCOIC) by managing and providing advice on cyberspace and computer network operations which support the organization's primary mission to ensure effective management, readiness, security and oversight of the Army's portion of the Department of Defense Information Network (DODIN). Provides mission management and technical

advisory support in the conduct of cyber network operations in support of the Army's offensive cyber operations worldwide, as required by the ARCYBER G33. Identifies cyber resources to facilitate and enables cyber tactical units. Provides a wide range of substantive oral and written presentations and reports to General Officer and DoD executive level officials. Briefs High-Level Officers and executive level officials and contributes to the development of Offensive CYBER Operations (OCO) policies for CYBER Space operations. Maintains relationships, interfaces, and coordinates with Intelligence Community, Defense Agencies, Joint Staff, Government Agencies, Law Enforcement, and Network Operations (NetOps) Communities. Supports both offensive and defensive targeting efforts for ARCYBER. Primary focus is on nation states, non state actors, criminal & terrorist organizations, hackers, crackers and other threat actors operating within the ARCYBER global area of responsibility (AOR) with respect to CYBER targeting efforts. Analyzes congressional legislation, policy, guidance, doctrine, goals and objectives from DoD, JS, NSA and other military departments/agencies, for impact and implication on ARCYBER Offensive CYBER Operations (OCO). Maintains overall expertise on the capabilities and intentions of threat actors operating in the global AOR. Focuses on High Value Targets (HVTs), military capabilities, strategy, doctrine, tactics, techniques and procedures of these organizations and how they affect the internal stability of the host nation governments. Researches, analyzes, produces, and manages high quality in-depth assessments on issues of concern to the ARCYBER leadership. Identifies significant intelligence and targeting trends and proposes new or revised analytical efforts to alert key leaders to new developments to meet command requirements; based on analysis of all available intelligence requirements to fill gaps, and evaluates the intelligence collected in response to Information Operations (IO), Special Technical Operations (STO) and Cyberspace Operations requirements. Mastery of, and skill in applying: information systems security principles and concepts; sufficient to implement higher level security requirements such as those resulting from laws, regulations, or Presidential directives. Knowledge and mastery of the latest and most advanced techniques, procedures, concepts, principles, practices (encryption/de-encryption keying, communications connectivity and interface devices) applicable to secure configurations for restricted access and

counter measures for maintenance of the integrity of internal, external, wireless, and virtual computer-based networks. Broad knowledge of a wide range of information system vulnerabilities and protection concepts, principles, and practices to review, analyze and resolve difficult and complex security problems involving multiple integrated network systems for classified and unclassified security levels. Possess the ability to grasp, and interpret Department of Defense (DoD), Office of the Secretary of Defense (OSD), Organizations Officer of the Joint Chiefs of Staff (JCS), and military services doctrine, regulations, and procedures for the conduct of operations of CPTs and other elements engaged in computer network defense/cyberspace defense and incident response. Provides unclassified and classified briefings and analysis on complex, wide-ranging issues and topics from Strategic to Tactical level mission area analyses to identify cyber resources required to effectively support ARCYBER, National Security Agency, United States Cyber Command, or Combatant Commands requirements. As an Information Technology Specialist (Information Security), performed the following duties: Significantly contributed to improving the operations of the G-33's Offensive Cyber Operations. Key contributor to G-33 Offensive Cyber Operations (OCO) section's effectiveness and ability to provide timely and accurate reporting (OCO) section by developing processes, procedures and providing situation awareness to senior leaders. Effectively produces quality products which meet and often exceed the standard. Recognizes the value of coordination and synchronization across offensive operations and help to coordinate external visits with key stake holders to include U.S. Cyber Command and JFHQ-Cyber. Serves as the Cyber operations specialist for the U.S. Army Cyber Command as it conducts cyber operations in support of full spectrum military requirements and operations. Manages and provide advice on cyberspace and computer network operations which support the organization's primary mission. Provides advise and instructs on matters concerning the Army's offensive cyber operations worldwide. IT Specialist (Network/InfoSec) GS-12 UNITED STATES ARMY - Fort Gordon, GA October 2015 to January 2017 Responsible for the IT systems concept and capability phase of the system development life-cycle. Analyzed user Cyber needs and requirements to plan system architecture; translated proposed Cyber technical solutions into technical specifications;

evaluated interface between hardware and software and operational and performance requirements of overall system; documented design specifications, installation instructions, and other system-related information. Collaborated with system developers to select solutions and ensure compatibility of system components; evaluated current or emerging technologies to consider factors such as cost, security, compatibility, or usability; developed a system security context, a preliminary system security CONOPS, and defined baseline system security requirements in accordance with applicable IA requirements; evaluated security architectures and designed to determine the adequacy of security design. Provided guidance to team members in terms of policy and technical direction, performed long range planning of technical branch activities, monitored and coordinated efforts of contractors. Conducted defensive cyber operations as a host analyst during Operation Gliding Krypton, participated in the deployment and execution of the new Cyber tools with remote operations; brought back lessons learned to team to improve processes and Tactical & Technical Procedures for the 151 Cyber Protection Team (CPT) future Cyber technologies deployments and remote operations. Improved and maintained multiple tactics techniques and procedures (TTP) used for Host team analysis, covering a multitude of tools and applications, assisted with automating and standardizing mission deliverables. Assisted with the development and presentation of the risk mitigation plan for OAK, enabled C2 support the ability to limit them of a cyberattack to surface and mitigated system vulnerabilities. Cyber Security Engineer Contractor UNITED STATES ARMY - Fort Gordon, GA June 2015 to September 2015 Provided support of INSCOM Information Assurance and Security mission at Fort Gordon, GA. Assisted in the development and implementation of INSCOM information assurance and network security courses of actions. Generated required systems security plans, designs, and reports in accordance with DIACAP and Intelligence Community Directives to include (ICD) 503, DCID 6/3 and the NIST Risk Management Framework. Worked with stakeholders to define and analyze system security requirements and provide technical solutions to best fit the customers' needs. Applied Information Assurance (IA) principles during all phases of the system development lifecycle and conduct internal audits to ensure compliance with current DoD and Intelligence Community Security directives, policies, regulations, guidance, security

technical implementation guides, and industry security best practices. Served as Information Assurance Network Manager for the Agency. Coordinated with Agency managers and with external counterparts and industry representatives. Anticipated the effects of new emerging technology and developed policies to control it to prevent security violations. Duties included oversight of all information systems, hardware and software, and accreditation of all systems IAW AR 380-19. Ensured that all Agency employees follow guidance concerning accreditation of automated information systems, risk management, control of computer viruses, continuity of operations plans (COOP), and other similar issues. The incumbent had a program oversight responsibility for the Installation Campus Area Network (ICAN)/Local Area Network (LAN) Certification and Accreditation (C&A), documentation and meets AR 25-1, AR 25-2, DoDI 8500.01 (Cybersecurity) and DoDI 8510.01 (Risk Management Framework (RMF) for DoD Information Technology), as well as the legacy C&A guidance procedures under DoDI 8510.01 (DoD IT Defense Information Assurance Certification and Accreditation Process (DIACAP)) and DoDI 8500.2 Information Assurance (IA) Implementation. Ensured that a wide variety of security incidents are investigated and reported IAW AR 25-2 and DOD O-8530.1 to include: computer viruses, and sanitation of highly classified information. Led the 513th MI BDE's CITRIX Accreditation by implementing of NIST Risk Management Framework Process through the DoD Enterprise Mission Assurance Support Service (eMASS) information system Certification and Accreditation Process. Performed Public Key Infrastructure (PKI) spot security inspections of Registration Authority/Local Registration Authority (RA/LRA) workstations, workspaces, and reviewed RA/LRA audit and system logs. Information Systems Management Officer UNITED STATES ARMY- HHC - Fort Gordon, GA April 2012 to March 2015 Manages the planning, engineering, installation, operation, maintenance, and defense of a highly sensitive secured Department of Defense global communications network with 30+ Points of Presence and 100 communications assemblages. Manages organizational Information Management training programs and oversees the Army Training and Certification Tracking System (ATCTS) and IA/CND/Cyber Security training. Advises senior executive leadership on network security operations and responsible for the consolidation and trending of cyber incidents and the

creation of products to be used for briefing leadership, partners, and customers regarding computer network defense. Led a specialized Network Defense team of 5 network and enabled continuous 24-hour communications during redeployment of 400+ personnel from Afghanistan to the United States. Developed and implemented Cyber Security Standard Operations Procedures, Continuity of Operations (COOP), COMSEC material, and awareness training throughout the unit. Led the implementation of NIST Risk Management Framework replacing the DoD Information Assurance Certification and Accreditation Process (DIACAP), a plan of action and milestones (POA&M), Incident Response Team Lead, and manages the life-cycle Cyber Security risk to DoD IT validation requirements and in compliance with FISMA. Managed the acquisition and procurement of life cycle replacements of automations equipment and software supported an organization of 3,000+ users. Plans & Operations Officer UNITED STATES ARMY - East Point, GA May 2009 to June 2011 Coordinated communications and automations support for 8200+ personnel geographically dispersed throughout the United States. Consulted with subordinate business units to monitor, assist and provide guidance on the unit's mobilization readiness. Developed the organizational Mobilization Readiness Update Brief that maintained situational awareness for senior executives during deployment preparation. Led the Operational Support Team during the 335 Signal Command Regional Training Center rotations at Fort Dix, New Jersey. Information Systems Officer U.S. Army January 2007 to May 2009 Supervised deployable communications assets for US Southern Command Joint Task Force Bravo (JTF-Bravo) supporting 1200+ US personnel conducting multi-national partnership operations in Central and South America. Managed the operation and maintenance of telephone, radio and tactical satellite communications systems and the unit's only deployable flyaway kit valued more than $2M. Supervised Network Defense Team the daily operations of the JTF-Bravo Communication Security vault, Continuity of Operations (COOP), and ensured 24-hour continuity of telecommunications support. As COMSEC Custodian planned and organized personnel and resources to achieve a 400% reduction of communication security incidents during a Communication Security Logistics Activity audit, becoming recognized as the US Southern Command's Communication Security Subject Matter Expert. Upgraded Communication

Security assets through the acquisition and integration of 80 new Key Security Verbal-21 encryption devices that improved the task force's ability to meet secure voice communications. Designed and implemented a Communication Security training program that trained 90 personnel to maintain continuity and 100% accountability of classified systems during period of high personnel turnover. Performed economic Cost-Benefit Analyses utilized by senior officials in the planning, programming and budgeting of automation resource requirements. Telecommunication OPS Chief UNITED STATES ARMY March 1988 to December 2006 Expeditionary Signal Platoon Sergeant in an Expeditionary Signal Company; responsible for the installation, operation and maintenance of 5 AN/TRC (Army-Navy/Transportable Radio Component)-190(V1), 2 AN/TRC (Army-Navy/Transportable Radio Component)-190(V3) Line of Site (LOS) transmission systems, 1 AN/TSC (Transportable Satellite Component)-93 multi-channel hub satellite terminal, 5 Command Post Node (CPN) teams, 1 Joint Node Network (JNN) team, 1 cable and wire team, all associated trailers, vehicles and power generation equipment worth over 7.5 million dollars; responsible for the morale, welfare, training, discipline, and safety of over 54 Soldiers. Education Master of Arts in Information Technology Management in Information Technology Management Webster University 2013 Bachelor of Arts in Business Administration in Business Administration Saint Leo University 2011 Skills Training, Security, Sharepoint, Web design, Cissp, Comsec, Pki, Active directory, Ccna, Cisco, Exchange, Firewalls, Networking, Virtualization, Nessus, Network monitoring, Internet explorer, Sql server, Sql server 2005, Sql Links http://linkedin.com/in/edibertomera Additional Information TECHNICAL SKILLS Certified Network Defense Architect, Computer Network Exploitation, CNO Attack & Defend, CNO Capabilities Developer, Malicious Network Analyst, Cyber Threats Analyst, Mission Protection Squad, LINUX Essentials, CCNA, CISSP, CISCO Security, Firewalls, Network Monitoring Windows 2008 Server, Windows Server 2008 Network Infrastructure, MS Active Directory Infrastructure MS Win7, MS Office 2007, MS Exchange, MS Outlook, MS Internet Explorer SharePoint 2010, Web Design, SQL Server 2005, Adobe Connect, Virtualization NSS PKI Trusted Agent, Army Incident Handling Virtual Training Course, Social Networking v1.0 Virtual training, COMSEC Custodian, Local COMSEC Management Software (LCMS), Assured

Compliance Assessment Solution (ACAS), Enterprise Mission Assurance Support Service (eMASS), Host Based Security Systems (HBSS) Policy Writer, Nessus Vulnerability Scanner, Continuous Monitoring & Risk Scoring (CMRS)

Name: Maurice Flores

Email: stewartsamuel@example.org

Phone: +1-905-944-4554x349