ISRAEL BRIGGS, MBA,CISSP, CMMC CA

(202) 596-2022 – *Israel.briggs@b2cybernetics.com*

US Citizen - TS-SCI and Q Cleared

Professional Experience

B2Cybernetics 1/18 –

Cyber Security Consultant/Assessor Remote

- Provided 3rd party and self-assessment (FedRAMP, CMMC, GLBA, HIPAA, RMF) support to audit companies and government primes.
- Provided cyber security consulting services to consulting companies and government primes.
- Facilitated tabletop exercises
- Facilitated scoping workshops
- Assessed High and Moderate systems to achieve authorized system use including common controls and FedRAMP systems for Y-12 and Pantex locations.
- Developed profiles in Archer for multiple systems ensuring Agency head and ISO remained compliant with Federal Information Security Modernization Act and respective DOE mandates.
- Developed Baseline and Risk Assessments for subsystems.
- Performed ISSO duties for 14 systems including: Perform system categorization, create ATO packages and artifacts and create Risk assessment report and enclaving together in different ATO's.
- Interfaced with system SMEs to build system security plans.
- Reviewed system scans and STIGS.
- Mentor for junior SCAs.
- Assessed High and Moderate systems to achieve authorized system use.
- Conducted Readiness Assessments on all assigned systems slated ATO assessment.
- Developed profiles in eMASS for multiple systems ensuring Agency head and ISO remained compliant with Federal Information Security Modernization Act and respective DoD mandates.
- ATO: ISSM for 25 systems: Perform system categorization, create ATO packages and artifacts and create Risk assessment report and enclaving together in different ATO's.
- Initiated effort to compile list of commonly applicable impact statements to be used as reference for POA&Ms, designed to minimize the POA&M authorization time in eMASS and standardize ISSM team language.
- Saved the Agency approximately $200k by debunking an assumed limiting factor in the system's design, guiding the agency to most appropriate, economic and compliant course of action.
- Review control implementation statements (CCI's) for compliance to run thick skins to make sure hardware is aligned with NIST 800 53 controls.
- Developed DoDM 8570 Compliance tracker tool that was implemented for all DLA OT portfolio systems providing assigned Program Managers the ability to easily ensure compliance with DoD personnel mandate requirements and decreasing dependency on ISSM team.
- Developed NIST SP 800-60 Data Type Identifier tool that is slated for implementation for all DLA OT portfolio systems providing assigned Information System Owners the ability to effectively identify data requirements resulting in accurate system categorizations and decreasing dependency on ISSM team.
- Responded to numerous incidents identified by DLA CERT team, assisting with follow-on investigation, evidence gathering and chain of custody and forensic analysis, resulting in the identification and removal of two rogue ISP devices and discovery/eradication of 17 advance persistent threats.

- Hand picked to assist in the development of a System Security Plan template customized for the Operational Technology portfolio allowing a clear path to authorization for DLA's vast number of "break fix" OT systems.

Knight Point Solutions 08/18 - 01/20
ISSO Remote

- Assigned Information System Security Officer for DHS's Xacta instance.
- Conduct readiness assessments on all assigned systems slated for ATO assessment.
- Provided information system security officer support for 8 Department of Homeland Security systems, including 3 "high-vis" systems and even DHS's XACTA system.
- Led system level Change Control board for assigned systems and participates when necessary in ISO CCB, to include creating and presenting formal Change Requests.
- Assisted Agency to secure ATOs for SaaS Cloud Solution's through FedRAMP inheritance, securing ATO 6 months ahead of schedule.
- Selected applicable system security controls and tailored out those not applicable in DHS's risk management system Xacta resulting in acquiring ATO two months ahead of schedule.
- Regularly interfaced with SOC to implement hardening configurations and patch vulnerabilities, identified and remedied the Agency's use of outdated STIG scan profiles.
- Utilized Nessus Security Center to validate presence of vulnerabilities on assigned systems and created reports and dashboards, maintaining a cybersecurity metrics score card average of 95% my entire tenure.
- Utilized Splunk to analyze data for investigations on assigned systems, monitor and created reports and dashboards. Created over 20 Splunk scripts resulting in automated monitoring and reporting of vulnerabilities and indicators of compromise allowing me to manage more systems at once than any other member of the team.
- Made strong, clear and articulate cases advocating System Owners to waive certain control requirements when assumed risk was at acceptable levels to expedited ATO process allowing System Owners to trim 20% of controls off applicable baselines on average.

Qualis Corp 11/17 - 05/18
ISSM Eglin AFB, FL

- Conducted Readiness Assessments on all assigned systems slated ATO assessment.
- Protected information and prevented unauthorized access by researching, developing, implementing, testing, and reviewing hardware/software information security requirements (IAW DoD/NIST RMF).
- Managed controls through eMASS to include coordinating to establish accounts and profiles, control selection, artifact entry, POA&M managing and the submitting of control inheritance requests and packages for assessment. Registered PPS in the DoD Central Registry and processed all PPSM requests assuring compliance with DoD Instruction 8551.1 through the Air Force PPS Office, with requests being completed, submitted and processed in under 10 days.
- Developed and reviewed existing system-specific Security Controls Test Matrix (SCTM), Risk Assessment Report, Plan of Action and Milestones (POA&M), System Security Plans (SSP), Application Security and Development Checklists, and other artifacts supporting software certification and accreditation in accordance with RMF and JSIG identifying areas for Enterprise Cybersecurity & Cyber Resiliency opportunities for improvement
- Hardened Operating Systems, applications, and network infrastructure using Department of Defense Security Requirement Guides (SRGs), Security Technical Implementation Guides (STIGs), Defense Security Service Office of the Designated Approving Authority (DSS ODAA) Baseline Technical Security Configurations, and Information Assurance Vulnerability Alerts (IAVA) resulting in full remediation of 96% of all identified vulnerabilities on assigned systems during tenure.

Marathon TS 09/17 - 11/17

Security Control Assessor Representative Gunter-Maxwell Annex, AL

- Specifically requested by previous employer's Prime to join SCAR team, assessing systems and validating controls for Air Force Life Cycle Management Center.
- Produced 4 SARs and advised the AODR on government system risk status resulting in 4 complete assessments and 4 ATO certifications/re-certifications.
- Reviewed artifacts through eMASS, validating over 1000 compliance claims in under 4 months.

PCI 05/17 - 09/17

Information System Security Officer Gunter-Maxwell Annex, AL

- Conducted Readiness Assessments on all assigned systems slated ATO assessment.
- Directed risk, compliance and security operations as described in DoDI 8510.01 in support of Air Force Life Cycle Management Center.
- Lead incident response efforts for assigned systems including forensic analysis.
- Developed IT Security Governance structure to reduce risks in organization processes, enhanced information security, and complied with regulatory requirements.
- Provided RMF, DIACAP, DISA Security Technical implementation guidance; prepared design specifications (e.g. network topology) for systems via Visio.
- Managed controls through eMASS to include control selection, artifact entry, submitting control inheritance requests.
- Fostered a change in culture that embraced new and challenging security requirements by improving communication and education.

STG, Inc. 10/16 - 05/17

Senior Network Engineer Gunter-Maxwell Annex, AL

- Served as an advisor to the Program Manager on all matters relating to network security vulnerabilities and threats to NCC computer systems, identifying 260 vulnerabilities and two confirmed indicators of compromise.
- Redesigned and lead military infrastructure team's restructuring of LAN, reconfiguring over 80 devices and reworking 20 comm rooms and reducing vlans from 74 to 12.
- Lead engineer on Solar Winds implementation project, completing project in 3 months providing complete network visibility.
- Initiated development of virtual network testing environment, project completed in 5 months allowing NCC the capability to simulated proposed network changes.

Military Reserve Experience

US Air Force Reserve 05/12 - Present

Director of Communication | Cyops Crew Commander | Cyber Officer Instructor KAFB/Gunter-Maxwell, AL

- Plans and coordinates USSOUTHCOM cyber exercises.
- Fully qualified AF Cyber Officer Instructor Augmentee, providing temporary instructor support for Offensive Cyber Operations, Defensive Cyber Operations, Threat Hunting, Linux and Windows courses.
- Specifically requested to augment Second Numbered Air Force's vacant Communications Director position and stand up their A6 Cyber Division during their re-org.
- AODR for 2 NAF reviewed Security Assessment Reports and made recommendations to AETC Authorizing Official for 9 systems, yielding 8 ATOs for 2 NAF
- Authored division mission/tenets resulting in a division structure created in-line w/AETC/Commander's directives and intent

- Action Officer diplomat; 1st of A-staff to conduct site visit since reorganization mandate resulting in the 1st AETC A6/2 AF Memorandum of Agreement
- Developed/deployed 1st 2 AF/A6 project tracker for 31 projects resulting in tracker considered for 2 AF/A3/maximizing 5,000 man-hours over four months.
- Cross trained team on CST functions resulting 2 AF HQ CST support increasing by 300% and secured more than $10K in training funds to train HQ A6 personnel in first week of arrival.
- Lead AFINC weapon system engagement; investigated over 4000 network events as a result crew successfully traced, sourced and prevented potential rogue actor attacks.
- Serve as team lead of 30 members for mission SMOKEJACK ALIB. Together we prevented and denied 30 hostile cyber attacks as a result our efforts achieved 24th Number AF's #1 priority and 4-star General visibility.
  Directed 4 Air Force Gateway maneuvers; mitigated service outage/degradation for 40 bases, assured mission capes for 845,000 AFNET users.
- Lead first Air Force Reserve Command (AFRC) Cyber Large Force Engagement as Mission Commander over 7 cyber squadrons. Expanded Indicator of Compromise (IOC) list based on personal knowledge of protocols which yielded more than a 6000% increase of positive hits in comparison to those yielded from the first search based on initial recon.
- Utilize Solarwinds to create status reports as well as creates new dashboard requirements to meet evolving mission requirements.
- Direct Event Controllers (EC) operations, including but not limited to oversight and coordination of EC mission readiness, establishing priorities for each shift, coordinate work schedules, evaluate work performance of subordinates, proper execution of DoDIN tasks and personal/professional mentorship and development.
- Hand-selected for JRSS Migration Tiger Team, a dynamic team stood up to ensure operational readiness in the remaining days to migration, revised processes, trained operators on new JRSS tools and demonstrated operational effectiveness during Air Force OUE (Operational Utility Evaluation).

Education & Certificates

- Troy University - Masters (Info Systems Mgt) 2015
- CMMC Lead CCA 2024
- CMMC CCP 2022
- eMASS CBT Certificate 2017
- NIST RMF Online Course Certification (Federal Cybersecurity Requirements) 2016
- ISC2 CISSP 2019
- Splunk Power User Certificate 2019
- Cisco Certified Network Professional Enterprise 2016
- SANS GIAC Certified Forensics Analyst 2019
- CWO (Cyber Warfare Operations) USAF Curriculum 2019
- Cyber 200 USAF Curriculum 2017
- CDCO (Cyber Defense Counter Offense) USAF Curriculum 2017
- UCT (Undergraduate Cyber Training) USAF Curriculum 2015
- Microsoft (Cloud) 365 Security Administrator 2020
- ITIL Foundation Certificate 2018
- ISACA Certified Information Security Manager CISM 2017
- CompTIA Certified Advance Security Practitioner 2017

Affliliations

- Court Appointed Special Advocate (CASA) of Harrison County

- ISACA
- ISC2
- Habitat For Humanity
- Reserve Officers Association

Technical Skills

- Forensic Analysis
- Metasploit
- Security Authorization Tools/GRC Plaforms: eMass, XACTA, ACAS
- Security Assessment Tools: Nessus, SCAP, STIG, Splunk, Claroty, WireShark, McFee, Tenable Nessus
  Specializations: NIST, FedRAMP, FISMA, DFARS, RMF, CMMC
- Cloud Solutions: MS Office 365, MS Azure, AWS Federal, GovCloud
- Software Applications: MS Project, MS Visio, MS SharePoint, MS Office Suite, MS Teams, MS Onenote, Adobe
- NIST 800 series: 800.53. rev 4, 800.18, 800.37, 800.30, 800.66, 800-60, 800-82
- ATO: ATO packages, mapping artifacts against NIST framework
- Languages: C, C++
- Operating Systems: Windows XP, Vista, 7, 8 & 10, Unix OS's, AWS OS's
- Software Applications: Microsoft Office (Word, Excel, PowerPoint, Outlook), G-Suite
- Tools: USCERT's CSET, Snip Tool
- Server NOS: Windows 2016/2012 R2, Windows2008 R2, Windows 2003/2000, NT Server 4.0, RedHat Linux, CentOS ● Email Servers: Exchange 2013/2010/2007, Office 365
- Web Servers: IIS 7.0/5.0, Apache 2.0.49 for UNIX/Linux
- Hardware: Server (HP, DELL, IBM), Cisco Meraki AP, Cisco Routers and Switches, network cards, printers
- Protocols: DHCP, DNS, SNMP, POP3, TCP/IP, TCP, UDP, ARP, SMTP, HTTP, FTP, TFTP, BOOTP, IMAP4, IPSec, MAPI
- Security Tools: Router, Cisco ASA Firewall, Fortigate Firewall; Bluecoat Proxy, VPN, IPSec, PPTP, L2TP
- Database: MS SQL 2014/2008/2005/2000/6.5, MySQL, MS Access 2000
- Languages: C/C++
- Scripting: Windows PowerShell 3.0, Python
- Systems Administration/other: Solarwinds NPM
- Cloud Solutions: Office 365, Microsoft Azure, AWS