Toli Georgoulis

2269 Kings Palace Dr

Riverview, FL 33578 Cell: (813)-843-5717

E-mail: toli.geotelecom@yahoo.com

NIST-RMF-DIACAP /FIPS/NIAP/NSA/DOE-FINANCIAL-BANKING Cyber Security - C4ISR Systems Engineering

Information Assurance System Security Engineer (IASSE)

**Prefer ONLY contract work; C2C. Prefer South East of USA, especially Tampa area, Fl. or SC/NC, or work remote from Tampa Fl & some travelling.**

EXPERIENCE SUMMARY:

Fifteen years of extensive and diverse military, civilian, technical, nuclear, financial/banking, training, and supervisory experience gained on a variety of command, control, communications, computer, intelligence, surveillance, Cyber Security and reconnaissance (*C4ISR*) systems and subsystems.

Well versatile on Certification & Accreditation via **NIST 800-37/53r4/ NIST 800-18, FISMA, NIAP/NISPOM, FIPS-199/200, Common Criteria (CC),**  **Financial & Banking, PCI**, **DIACAP-RMF/DCID-6/3, NERC CIP 002-011/14 & NEI 08-09/NAP14-1.D standards, NSA** **Type ½ Crypto, FIPS 140-2 crypto,** Lead customer Intelligence Driven Defense (IDD) methodology based incident response and analysis providing guidance to the customer on how to apply. Analyzes and re-engineers business processes to solve complex problems. Developed high-level design documents.for some of the following enterprise systems:

1. Information Systems (**IS**), Intelligence, **Nuclear Power Grid** Systems, **Gas & Oil Bulk Electric Systems**, **Federal & State** systems, **Financial & Banking** systems, **Surveillance and Reconnaissance Aircraft, Missile Defense Systems,** Meteorological and Weather Systems, Naval Weapon Systems, Telemetry, Navigational Aids (**NAVAIDS**), Satellite Communications (**SATCOM**). Security Compliance, Policies and Procedures Development, Risk Management, Security Assessments, etc.
2. **Experience with Procedure Development for the DOE - Department of Energy: Working on the transition of NERC CIP regulations version 3 & 5. Versatile with all the NERC CIP 002-011/14 Standards. Responsible for assisting Power Generation in the development, implementation, and communication of the information security practices, policies via NEI 08-09/NAP14-1.D, NIST SP 800-30/53r4,** and procedures which promote a secure and uninterrupted operation of Power Generation Industrial Control and **SCADA** systems(e.g. Emerson, Siemens, Honeywell etc.). Developing Critical Digital Asset (CDA) Assessments, Risk Management Assessment, mitigation, and implementation), Commercial Items (CI) and Non Developmental items (NDI), Disaster Recovery, Business Continuity Planning, Change Management, Configuration Management, and Network Management.
3. Airborne Communication Systems, Air Traffic Control (*ATC*) Communications, Avionics, and Instrumentation Systems, Command and Control Centers (Missile Range Mission Flight Control Centers), Ground Radio Communications Systems, (Point-to-Point, Ground-to-Air, Air-to-Air, and Air-to-Ground, Airport Electronics and Communications, Automated Information Systems (AIS),

1. Foreign Affairs Handbooks (FAHs), Foreign Affairs Manuals (FAMs) and DoS IRM/IA C&A Tool Kit, CNSSI 1253; NIST Special Publications (SPs) including **SP 800-30/53r4** and **SP800-37 / SP800-37 Rev 1**. National Security Agency (NSA) Certification & Accreditation for Type-1, 2& 3 Cryptosystems, and security appliances.

1. Secure Configuration Compliance Validation Initiative (SCCVI), GOLD Disk, Feasibility and Trade Studies. COMPUSEC, COMSEC (AR 380-41, 380-5, 380-19, and 380-40), ELSEC, EMSEC (AFM 33-214, AFI 33-203, NSTISSM/TEMPEST 1-95/2-95, 7010), INFOSEC, NISPOM, OPSEC, TRANSEC, and TEMPEST. Requirements definition, tracking and monitoring, Dynamic Object Oriented Requirements System (DOORS).

SECURITY CLEARANCE:

* Department of Defense (DoD) clearance: Active Secret clearance: Granted April 1983. Updated Feb. 2012. Interim/Judicated TS.

EDUCATION;

* BSEE in Electrical Eng., Athens, Greece 1975,
* BSEE in Electronics Eng., New York Institute of Technology, N.Y. 1976,
* MS in Digital Comm./Protocols, Brooklyn Poly, N.Y.
* Holding various certifications e.g. Net+, Sec+, SCH, CISSP, IAT Level III, CE, Security Certified Network Architect (SCNA), Certified Information Security Manager (CISM), CISCO certifications, NERC CIP Cert, and DISA Certs.

WORK EXPERIENCE:

NASA-Kennedy Space Center; NIST-RMF-DIACAP; NIST 800-37/53r4/FIPS199/200 Certification & Accreditation of various Network Systems and Industrial Control Systems (ICSs).

Lead Cyber Security Information Assurance Analyst/Consultant; 1-2017 to present…

**Application of the NIST/DIACAP/FIPS/FISMA Standards to produce Polices & Procedures for the entire NASA. Risk Management Framework (RMF), Risk Analysis and Mitigation Techniques via STIGS to harden Servers, (Windows, Unix, OSX, IOS and other infrastructure device OS),** (IDS/IPS), Identity Access Management (IAM), Role based access controls (RBAC), Applications Security(AppSec), Firewalls & Log Analysis, SIEM management Tool, Industrial Defender(ID), FoxGuard, Network Behavior Analysis tools, understanding of attack signatures, tactics, techniques and procedures associated with advanced threats.

**Perform Cyber Security Assessments on NASAs Critical Digital Assets (CDA) according to NEI 08-09 Cyber System Security Plan (SSP) for Nuclear Reactors, Gas & Oil Bulk Electric Systems with the 10CFR73.54 the NIST SP 800-3753r4 Standards and NERC CIP regulations version 3 to 5 transition. Working on the transition of NERC CIP regulations version 3 to 5. Versatile working with all the NERC CIP 002-011/14 Standards. Responsible for assisting Power Generation in the development, implementation, and communication of the information security practices, policies via NEI 08-09/NAP14-1.D, NIST SP 800-30/53r4, Cyber Security Policies(CSP) and procedures which promote a secure and uninterrupted operation of Power Generation Industrial Control and SCADA systems(e.g. Emerson, Siemens, Honeywell etc.).**

Apply all the NIST 800-53r4/DIACAP-RMF Information Assurance Controls to all the Systems to be accredited. Mapped all the NIST 800-53 Controls with the appropriate RMF and Common Criteria (CC) IA controls. Developed extensively all the necessary NIACAP artifacts (System Implementation Plan (SIP), NIST Implementation Plan (NIP), NIST Scorecard, IT POA&M/Corrective Action Plan) and the System Security Plan (SSPor Information Security Plan) in order to certify the systems. The SSP(ISP) is been developed according to the NIST SP 800-18 and contains all the C&A Artifacts to Certify the systems.

Well familiar with Web-Applications involving Servers(2008, 2012), Web-App Servers, Cisco Routers & Switches Cisco Nexus 7000, Cisco 3750; 3850; 2900; 3900, Cisco ASA/PIX Firewalls, Databases{(SAN), SQL, Sequel, ASPEN, PowerBase}, VPNs, IDS/IPSs, Data Loss Prevention(DLP), PKI and Act. Dir.(AD), Security Information Event Management(SIEM), Systems Vulnerability Assessments, Privileged User Management(PUM), Antivirus, Load Balancers, and specialized Software to Interconnect with other State agencies. Significant role with a very healthy amount of visibility while taking part in both strategic and tactical initiatives of the Local & Global Network Infrastructure.

State of S. Carolina; Dep. of Social Services (DSS); NIST-RMF-DIACAP; NIST 800-37/53r4/FIPS199/200 Certification & Accreditation of various State systems.

Lead Cyber Security Information Assurance Analyst/Consultant; 4-2015 to 12-2016

**Certified & Accredited many of the Systems of the Dept. of the Social Services of S. Carolina. Small and complex Networks**, Web-Applications involving Servers(2008, 2012), Web-App Servers, Cisco Routers & Switches Cisco Nexus 7000, Cisco 3750; 3850; 2900; 3900, Cisco ASA/PIX Firewalls, Databases{(SAN), SQL, Sequel, ASPEN, PowerBase}, VPNs, IDS/IPSs, Data Loss Prevention(DLP), PKI and Act. Dir.(AD), Security Information Event Management(SIEM), Systems Vulnerability Assessments, Privileged User Management(PUM), Antivirus, Load Balancers, and specialized Software to Interconnect with other State agencies and the IRS via the IRS 1075 standard. Significant role with a very healthy amount of visibility while taking part in both strategic and tactical initiatives of the Local & Global Network Infrastructure.

**Application of the NIST/DIACAP/FIPS/FISMA Standards to produce Polices & Procedures for the entire State and Social Services. Risk Management Framework (RMF), Risk Analysis and Mitigation Techniques via STIGS to harden Servers, (Windows, Unix, OSX, IOS and other infrastructure device OS),** (IDS/IPS), Identity Access Management(IAM), Role based access controls(RBAC), Applications Security(AppSec), Firewalls & Log Analysis, SIEM management Tool, Industrial Defender(ID), FoxGuard, Network Behavior Analysis tools, understanding of attack signatures, tactics, techniques and procedures associated with advanced threats.

Perform detailed requirements gathering, compile business and functional design documents, create and execute test plans, and assist with user acceptance testing and end user training. Participate in the configuration of applications to meet business requirements & Interface between IT and the end-users during systems development. Developed complex reports for all levels of management. Lead customer Intelligence Driven Defense (IDD) methodology based incident response and analysis providing guidance to the customer on how to apply. Analyzes and re-engineers business processes to solve complex problems. Developed high-level design documents.

**Apply all the NIST 800-53r4/DIACAP-RMF Information Assurance Controls to all the Systems to be accredited. Mapped all the NIST 800-53 Controls with the appropriate RMF and Common Criteria (CC) IA controls. Developed extensively all the necessary NIACAP artifacts (System Implementation Plan (SIP), NIST Implementation Plan (NIP), NIST Scorecard, IT POA&M/Corrective Action Plan) and the System Security Plan (SSPor Information Security Plan) in order to certify the systems. The SSP(ISP) is been developed according to the NIST SP 800-18 and contains all the C&A Artifacts to Certify the systems.**

**Also worked with the Chief Information Officer to verify that all the Inherited Controls are covered from the State Security Plans (e.g. Disaster Plan, Contingency Plan, COOP, etc.). Worked with the Sr. IA Officer, the Certification & Accreditation Officers and the DAA to produce a Risk free System or close to it.** Worked in hardening the Operating Systems as needed according to Government & State **STIGS**. Developed Test Procedures to validate and verify Test Cases. Working closely with stakeholders and the Senior IT management team your focus will be on WAN/LAN, Wireless and Mobile Connectivity supporting the firm worldwide.

Exelon(BGE, PECO, Com-Ed) ; NEXTera(Florida Power & Light); NUCLEAR Power Plan, Point Beach, WI; Martin Plan, Okeechobee FL, Juno beach HQ; (Lead & PM Cyber Security Information Assurance consultant; NERC CIP transition v3 to v5version, NEI 08-09, Cyber Sec. Policy updates. 12/2013 3/2015

**Perform PM functions and working with FPL management to have a smooth Project schedule. Perform Cyber Security Assessments on Critical Digital Assets (CDA) according to NEI 08-09 Cyber System Security Plan (SSP) for Nuclear Reactors, Gas & Oil Bulk Electric Systems with the 10CFR73.54 the NIST SP 800-3753r4 Standards and NERC CIP regulations version 3 to 5 transition. Working on the transition of NERC CIP regulations version 3 to 5. Versatile working with all the NERC CIP 002-011/14 Standards. Responsible for assisting Power Generation in the development, implementation, and communication of the information security practices, policies via NEI 08-09/NAP14-1.D, NIST SP 800-30/53r4, Cyber Security Policies(CSP) and procedures which promote a secure and uninterrupted operation of Power Generation Industrial Control and SCADA systems(e.g. Emerson, Siemens, Honeywell etc.).**

Finished Assessment packages for various Critical and Non Critical Digital Assets (**CDAs**). Evaluating the Assets (CDAs), do walk arounds in the Core and outside the Radiation zones. Taking pictures of them and retrieving the appropriate drawings to determine the criticality of the Assets via the SP 800-53r4 IA Controls. Working with various **SIEM** tools, Security Information Event Management (SIEM), Industrial Defender(ID), Systems Vulnerability Assesment, Privileged User Management(PUM), e.tc. WinAudit – Freeware application for data collection, CatTools – Switch/Router Configuration, nCircle – Vulnerability Management, nFront – Password Complexity tool for windows cyber assets, nMap – Used to scanning ports and services, Password Safe – Used to document and store all passwords.

**Write Cyber Security Policies (CSP) via NEI 08-09/NAP14-1.D, NIST SP 800-30/53r4, and NERC CIP 002 to 009/10/11/14 procedures which promote a secure and uninterrupted operation of Power Generation Industrial Control and SCADA systems** e.g. Emerson. Working on the transition of the **CIP 03 to CIP 05** requirements. To support an efficient transition, FERC/NERC and the Regional Entities developed a compatibility table, referred to as the V3-V5 Compatibility Table, which lists each of the requirements in the CIP V5 Standards and identifies whether the requirement is: (a) compatible or mostly compatible with a requirement in the CIP V3 Standards; or (b) a requirement new to the CIP V5 Standards that does not correlate to a CIP V3 requirement.6 A CIP V5 requirement is compatible with a CIP V3 requirement where the content and compliance expectation of the CIP V5 requirement is substantively similar to a corresponding CIP V3 requirement.

Develop an Excel Check List to assess the applicability of the IA controls to each system. All IA Controls were answered as to their Compliance, the Non Compliance and their Non Applicability to each asset system along with their Threat Vectors. Confirming information acquired during tabletop reviews and walk-downs. Develop final assessment documents for each asset and working with the Nuclear Security engineers to approve the Assessments. Recommending as necessary remediation techniques to mitigate issues with the CDAs.

Aberdeen Proving Grounds (APG), ARMY’s C4ISR Center of Excellence, MD; (Lead Cyber Security Information Assurance consultant/analyst; NSA/DIACAP-RMF/NIST/FIPS/FIPS 140-2 etc.) 11/2010 to 11/2013

Supporting the ARMY’s C4ISR Center of Excellence for all Cyber Security IA programs. This involves the Crypto Modernization Program for most Crypto Units, Radios, and ANDROIDS, Cross Domain Solutions, JTRS radios(the new MNVR), JTRS Waveforms(especially the new WNW, MUOS & new SRW/EP), Handheld Radios, PDAs, HAIPE devices, Secure phones, Android Tablets & Smart Phones, via **NSA,** **FIPS 140-2**, **NIST/NIAP,** **DIACAP/Army Regulation 25-2.** Analysis of the IA controls, and generating all the **DIACAP-RMF/NIST** artifacts: **SIP, DIP, Scorecard, POA&M, Sys Sec Plan, Sec Test &Eval files for the C&A effort**; Deliver to customer the DIACAP/NIST packages for review and comments. Worked with DoD SRGs and DISA STIGs on the System Security Policy (Plan) for all Projects. Draft copies were generated for Gov. customer review. Worked with the Gov. representatives to resolve IA issues and finalize all the **DIACAP-RMF/NIST** C&A Packages for IATO/ATO.

Expertise in security of multiple operating systems, especially: HPUX, Linux, Windows, other OSs; access control, authorization and authentication technologies: PAM, Active Directory, LDAP. Securing fundamental networking protocols: **DNS, HTTP, TCP, UDP, TLS, IPSEC, 802.1x, NFS**. Encryption fundamentals techniques (symmetric/asymmetric, ECB/CBC operations, AES, etc.).

Worked with **NIST SP 800-30/37/61** & federal Gov. Security regulations, **NIST SP 800-53r4, NISPOM, DoD PKI & LDAP** etc.

Working with the Department of Energy Nuclear/DOE - NERC CIP regulations version 3 & 5. Responsible for assisting Power Generation in the development, implementation, and communication of the information security practices, policies, and procedures **NEI 08-09/****NAP14-1.D** which promote a secure and uninterrupted operation of Power Generation Industrial Control and SCADA systems. Security Information Event Management(SIEM), Systems Vulnerability Assesment, Privileged User Management(PUM), Identity Access Management(IAM), Role based access controls(RBAC), Applications Security(AppSec), Firewalls & Log Analysis,

Overseeing the Key Management Infrastructure (KMI) with the development of a Software Application (KMI2) to transfer Black Keys from KMI-MGC to flow into an existing ACES workstation down to the Brigade level.

Worked on the New SRW-EP Waveform for the Army and the New MNVR radio. Supporting all the IA & Security architecture and the overall HW/SW architectures including the Special Features, e.g. Advanced Routing, MIMO Project Management, Interference Cancellation, Directional Networking, EW Scenario development, etc. SRW-EP will run in Un-Classified and Classified mode. Supporting the COMSEC & TRANSEC issues with NSA and key Management.

Advanced C4I Solutions, Inc. Tampa, FL 11/2009 to 11/2010

Sr. Information Ass. Cyber Security Analyst/Consultant; DIACAP-RMF/NSA/NIST (3 locations)

1. EGLIN Air Force Base Ft. Walton Beach, FL. Air Combat Training

Leading the IA & Security team at Eglin Air Force base, FL for the **DIACAP-RMF** (**SIP, DIP, Scorecard, POA&M, Sys Sec Plan (SSP) & Sec Test & Eval)** Certification & Accreditation of the Air Combat Training Systems. The architecture involves air to ground radios, Aircraft processors, NSA Crypto devices (e.g. KG-250X HAIPE devices) and Cross Domain Solutions (CDSs). Also includes simulated weapons processors so the pilot can do training in a LIVE and SIMULATED environment up in the air. The training involves F-15s, F-18s, JSFs (F-35) and other NATO aircraft. This is a Multilevel Security domain Air Combat Training exercises. Expertise in security of multiple operating systems, especially: **HPUX, Linux, Windows, other OSs;** Expertise in access control, authorization and authentication technologies: PAM, Active Directory, LDAP. **Securing fundamental networking protocols: DNS, HTTP, TCP, UDP, TLS, IPSEC, 802.1x, NFS.**) Vulnerability assessment process and tools experience a strong plus: OWASP, Burp Suite, SpiDynamics, etc. Understanding of risk modeling concepts and frameworks e.g. STRIDE, DREAD, FAIR.Strong background in data driven information security decision making and prioritization; Strong understanding of the attacker kill chain.

Also leading the IA & Security of a Hand held device for an R&D Army/Marines project. Involved in the HW & SW architecture of the whole Hand-held and particularly in the Cyber Security architecture. Involved in customer and NSA meetings to further develop the DIACAP-RMF Certification & Accreditation of the system. The system involves an Android smart phone, a Crypto SUITE B engine and a Tactical Rifleman radio. The Android phone will run an ARMY application called FBCB2. This App is running in a secure OS environment. The smart phone provides user authentication via 2 factors and user roles. All messages back & forth to the Android are encrypted via a Type 3 FIPS 140-2 crypto engine.

2. United States Air Force Reserve Command (W. Robins, GA)

As a Senior Information Security Engineer, Mr. Georgoulis was the team lead for the United States Air Force Reserve Command (W. Robins, GA) supporting the Department of Defense Information Assurance **DIACAP-RMF** Certification and Accreditation (**SIP, DIP, Scorecard, SSP, POA&M files for the C&A effort)** activities of the Video Teleconference System; the Information Warning System (IWS), and various Telephone Switches. Responsibilities included registering DoD IS with Enterprise Information Technology Database Repository (EITDR/eMASS); developing DIACAP-RMF comprehensive and executive packages, System Security Plan (SSP), support documentation and artifacts; conducting security hardening using DISA STIGs, SRRs, and security checklists; Conducted independent verification and validation (IV&V), and security test and evaluation (ST&E) testing activities; conduct risk and vulnerability assessments, document, mitigate, and remediate deficiencies. Vulnerability assessment process and tools experience a strong plus: OWASP, Burp Suite, SpiDynamics, etc.

3. Missile Defense Agency, Spacelift Range System Contract (SLRSC)

As a Sr. Information Security Consultant, Mr. Georgoulis provided certification and accreditation support to the Spacelift Range System Contract (SLRSC) for the Vandenberg Air Force Base Telemetry Receiver Site (VTRS). Responsibilities include reworking DIACAP-RMF C&A packages (**SIP, DIP, Scorecard, POA&M files for the C&A effort)** including the **SSP**, and **ST&E**. Conducting ST&E testing and reviewing raw test data. Developing the Security, Test and Evaluation (ST&E) plan, test cases and generating reports. Develop DIACAP-RMF Comprehensive & Executive packages; support documentation and artifacts. Make recommendations and comments to improve the success rate for project documentation. Identify, review, document, verify, test, and validate IA controls, safeguards, and countermeasures.

Conduct peer reviews. Provide expert technical guidance, interpretation, and implementation oversight of applicable information security policies, processes, and practices to support continued operational availability and integrity for DOD information systems and IT processes e.g. security of multiple operating systems, especially: HPUX, Linux, Windows, other OSs; access control, authorization and authentication technologies.

Implementing IA Cyber Security via Operating Security Centers (OSC) such as Emerson, and Honeywell. DSPs, PLCs, PAM, Active Directory, LDAP. Securing fundamental networking protocols: DNS, HTTP, TCP, UDP, TLS, IPSEC, 802.1x, NFS Encryption fundamentals techniques (symmetric/asymmetric, ECB/CBC operations, AES, etc.)

General Dynamics (GD) Sterling Heights, MI

Sr. Information Ass. Cyber Security Consultant; DIACAP-RMF/NSA/NIST 12/2007 to 11/2009

As a Senior Information Assurance Engineer (Team Lead), Mr. Georgoulis supported the GDLS/GDC4S JTRS-HMS Project. He conducted Department of Defense Information Assurance Security Certification and Accreditation Process DIACAP-RMF via the (**SIP, DIP, Scorecard, Sys Sec Plan (SSP), POA&M files for the C&A effort and IATO/ATO)**; Vulnerability assessment process and tools: OWASP, Burp Suite, SpiDynamics, etc. Understanding of risk modeling concepts and frameworks e.g. STRIDE, DREAD, and FAIR. Strong background in data driven information security decision making and prioritization;

Strong understanding of the attacker kill chain activities for several platforms to include the JTRS-HMS radios (e.g. Rifleman (Type 2), Type 1 radios and the R&D HAIPE Type 1 Vehicle Radio (NSA Type 1 Certification & Accreditation); Also supported the Future Combat Systems (FCS), Abrams New Evolution Tank, Stryker Family of Vehicles, Joint Light Tactical Vehicles (JLTV) and MUOS waveform. Responsibilities include developing DITSCAP C&A packages, support documentation and artifacts; identifying and documenting security requirements; conducting security hardening activities using DISA and NSA Type 1 security technical implementation guides (STIGs), security readiness reviews (SRRs) and security checklists, and industry best practices. Conduct risk and vulnerability assessments IAW DISA PSSM/CAP policies and procedures; conduct independent verification and validation activities; conduct risk management activities (assessment, mitigation and remediation). Mr. Georgoulis was the subject matter expert for several Cross Domain Solutions (CDS), and for HAIPE Type 1 devices.

Rockwell Collins, Cedar Rapids, IA

Sr. Information Ass. Security Analyst/Consultant; DIACAP-RMF/NSA/NIST 03/2003 to 12/2007

As a Senior Information Assurance Engineer (Team Lead), Mr. Georgoulis supported the JTRS Ground Mobile Radio (GMR), Airborne Marine Fixed (AMF), and Future Combat Systems (FCS) project. Responsibilities included conducting NSA, NIACAP, DIACAP/NIST certification & accreditation packages. Conduct DITSCAP to DIACAP transitioning {Expertise in security of multiple operating systems, especially: HPUX, Linux, Windows, other OSs; access control, authorization and authentication technologies: PAM, Active Directory, LDAP. Securing fundamental networking protocols: DNS, HTTP, TCP, UDP, TLS, IPSEC, 802.1x, NFS. Encryption fundamentals techniques (symmetric/asymmetric, ECB/CBC operations, AES, etc.) Vulnerability assessment process and tools experience a strong plus: OWASP, Burp Suite, SpiDynamics, etc. Understanding of risk modeling concepts and frameworks e.g. STRIDE. Strong background in data driven information security decision making and prioritization; Strong understanding of the attacker kill chain. Conduct security test and evaluation, (ST&E), configuration, test and evaluation (CT&E), and independent verification and validation (IV&V) activities. Conduct risk and vulnerability assessments. Conduct risk management activities (assessment, mitigation and remediation). Conduct security hardening activities using DISA STIGs, SRRs, and security checklists. Develop C&A packages, support documentation and artifacts. Map security requirements to system requirements. Develop security test and evaluation test cases. Evaluate defense in-depth architecture and designs and made recommendations for improvements.

Raytheon Corp, St. Petersburg, FL

Sr. Information Security Lead 02/2001 to 03/2003

As an Information Assurance Engineer (Team Lead), Mr. Georgoulis supported the Multi-sensor Command and Control Aircraft platform (MC2A) with C4ISR (Intelligence, Surveillance and Reconnaissance) sensors and associated subsystems for the United States Air Force. Enter security requirements into the DOORS database. Develop DITSCAP certification and accreditation packages, support documentation and artifacts. Conduct security test and evaluation (ST&E) activities, and developed ST&E test cases. Conduct risk and vulnerability assessments. Conduct risk management activities (assessment, mitigation and remediation). Configure system components, and employ DISA/NSA STIGs.

Honeywell, Corp Columbia, MD

Information Security Consultant 05/1997 to 02/2001

As an Information Assurance Engineer (Team Lead), Mr. Georgoulis supported the FAA/NASA Aeronautical Telecommunication Network (ATN). Responsibilities included installing and configuring the public key infrastructure (PKI). Supervise a team of 10 IA engineers. Develop the Air to ground digital protocol (VDL M2) IAW OSI methodology utilizing ICAO VDL M2 and SARPS. Develop DITSCAP C&A packages, support documentation and artifacts. Develop ST&E plan, test cases, and conduct testing activities.

Northrop Grumman

Linthicum, MD; Sr. Systems Consultant 03/1991 to 04/1997

As a Senior System Engineer, Mr. Georgoulis supported the Air Traffic Control Division/Software Integration. Responsibilities included develop system design and architecture, and documentation. Defining system requirements and mapping requirements to system architecture. Conduct system and networking activities. Conduct network modeling and simulation activities, and coordinate and schedule system integration activities.

Emerson EL Corp., Software Test & Integration Division

Sanford, FL; Senior Systems Engineer 01/1986 to 02/1991

As a Senior System Engineer (Team Lead), Mr. Georgoulis Manage testing activities to Design with a team effort various test stations for DOD projects. The Test stations will test various LRUs, such as radars, radios, antennas, etc.