

Isiah Jones

Senior Principal Cyber Professional

Summary

Senior Principal Cyber Professional with 20 years of progressive experience in various aspects of information technology (IT), information systems (IS), information sciences, information security, information assurance (IA), mission assurance, industrial control systems (ICS), operational technology (OT), industrial internet of things (IIoT) and internet of things (IoT). 2004-2014 was primarily IT/IS/IA focused. Has been ICS OT IIoT IoT mission assurance, cybersecurity, national security, critical infrastructure, and safety focused since 2014.

Has performed work in the Middle East, East Africa, Europe, Hawaii, and throughout the continental United States. Has delivered cyber IT or ICS OT security services or support for the US Navy, US Marine Corps, NSA, Siemens, FERC, FHFA, US Patent & Trademark Office, and various private sector asset owners, product vendors, EPCs, system integrators and others. Has worked across several sectors and asset verticals such as defense industrial base including intelligence agencies, semiconductor radio communications manufacturing, pharma manufacturing, pulp, paper and consumer goods manufacturing, oil, gas, electric, buildings and facilities, maritime, water and wastewater etcetera. **DoD CAS tier 5 SSBI TS/SCI current and active as of March 2024.**

Understands the nuances of DoD cybersecurity policies including 8500.01-M, 8510.01, JSIG, CNSSI 1253, ICD 503, etcetera. Has an understanding and experience with tailoring the implementation of security controls for both traditional IT and nontraditional platform IT, embedded systems, automation, and control systems.

Areas of Expertise and Interest

- Cybersecurity IT and ICS OT IoT
- RMF, DIACAP, NIST (SP 800-53, 82, 160, CSF etc.), UFC 4-010-06, ISA/IEC 62443, ISA84.00.09, NERC CIP, MITRE ATT&CK for ICS
- Mission Assurance, Risk, Vulnerability, and Threat Assessments
- Vulnerability Management, Scanning, and Analysis
- Systems Design, Testing and Validation
- Factory Acceptance Test (FAT), Site Acceptance Test (SAT), User Acceptance Testing (UAT), Defect Testing, System Validation
- Data Visualization, Threat Modeling, and Attack Mapping
- Plan of Actions & Milestones (PO&AM) and Roadmaps
- Standards, Regulations, Directives, Orders, Memos, National Security
- SAP ERP
- Systems Analyst, Security Analyst, Information Assurance Officer (IAO) and Information Systems Security Engineer (ISSE)

Degrees & Certifications

Penn State University: Masters in
Homeland Security – Information
Security and Forensics
Penn State University: Bachelors in
Information Sciences and
Technology – Systems Integration &
Application
CompTIA Pentest+ce
Global Industrial Cyber Security
Professional (GICSP)
Certified Information Systems
Security Professional (CISSP)
CompTIA Security+ce
Intermediate US Navy Validator
(former)
OSHA 30 General Industry (expired)
Certified Chief Information Security
Officer (C|CISO) (expired)

LANGUAGES

English

Contact Info

- Resident location: Alexandria, VA •
Resume Update: 05/2024
- Cell: +1 717.364.0697
- Email:
isiah@icubedsolutionsllc.com

Relevant Experience

Employer: Applied Integrated Technologies Inc (AIT)

Title: Cyber Engineer (ICS OT IloT IoT Cyber-Physical) **(TS/SCI)** **Salary: \$210,000/yr. full-time**

Start/End Dates: August 2022- December 2023

Scope/Description: Cyber Engineer within the Cyber Mission Assurance Capabilities (CMAC) team providing ICS OT IloT IoT Cyber-Physical and Embedded component security engineering expertise and services. Implementing, assessing, and testing security requirements during FAT and SAT, equipment reverse engineering and mapping to ICS ATT&CK and ISA/IEC 62443, creating and executing product security services for secure design lifecycle maturity, red team and pentesting operations, security risk assessments and systems security engineering engagements. Supporting asset owners, integrators, engineering firms, OEMs as well as product and equipment vendors. Collaborating with standards organizations, sector organizations, and governments to improve standards, regulations, guidelines, tools, templates, education, and awareness of ICS OT IloT IoT Cyber-Physical and Embedded component security. Continuing to contribute to ISA84, ISA/IEC 62443, AWWA, PLC Top 20 Secure Coding practices and CISA CSAC Technical Advisory Council.

Tools: Kali, VirtualBox, AttifyOS and IoT exploitation kit, Tenable Nessus, OpenVAS, Object Security, RF SDR tools, Binary Ninja, Nmap, SonarQube, Azure DevOps, Office365 suite, Offensive Azure Cloudbreach tools, STIGs, and CIS Benchmarks, OWASP ZAP, The Harvester, Grassmarlin, etcetera.

Trainings: Physical Red Teaming, Attify IoT Exploitation and Pentesting, CloudBreach Breaching Azure, eMASS CBT 7.0, Practical ICS Penetration Testing, Azure A to Z, AZ-500 Azure Security, Tenable University various product courses, etcetera.

Employer: National Resilience Inc

Title: Principal Security Engineer – ICS Security Integration **Salary: \$200,000/yr. full-time**

Start/End Dates: October 2021 – August 2022

Scope/Description: Principal Security Engineer for ICS Security Integration within the Vendor & Supply Chain Risk department of the Digital Security Group. Leading secure by design implementation of company ICS security requirements into active and future brownfield and greenfield control systems and automation systems design build projects and daily plant manufacturing operations equipment and systems. Providing subject matter expertise, tools, self-service capabilities, methodology, templates, etcetera of standards and best practices for ICS OT security. Conducting as needed security configuration and testing during factory and or site acceptance tests, sandbox testing and ensuring functional design specs include security requirements (e.g., ISA/IEC 62443, PLC top 20 Secure coding practices). Collaborating with architecture and infrastructure teams to ensure correct security tools and firewall rules that are compatible with ICS OT manufacturing equipment are selected, installed, and configured in a way that will not cause operational equipment issues for ICS OT assets. Continuing to contribute to ISA84, ISA/IEC 62443, AWWA, PLC Top 20 Secure Coding practices and CISA CSAC Technical Advisory Council.

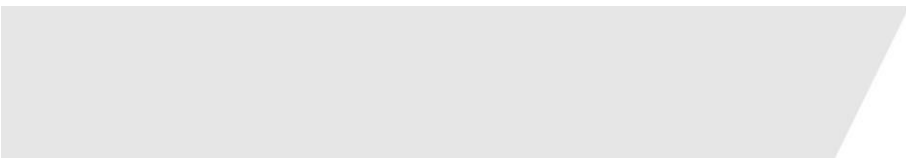
Tools: Tenable OT, Kali, Nmap, OpenRMF, STIGs, JIRA, Confluence, ServiceNow, Smartsheet, Box, Lucid Chart, Veeva, Ignition, VirtualBox, Airtable, etcetera.

Employer: Closedloop Communications Inc

Title: Control Systems Cybersecurity SME **(SSBI TS)** **Salary: \$185,000/yr. full-time**

Start/End Dates: July 2020 – October 2021

Scope/Description: Control Systems Cybersecurity SME with a range technical and non-technical SR level and hands on advisory, leadership, consultant and security engineer experiences supporting various customers including bringing in additional global ICS business and partners across several sectors. Providing Platform Resilience Mission Assessments (PRMA) ICS OT expertise for NSA Cyber Directorate, US Military Services



and Minerva/ManTech. Continuing to contribute to ISA84, ISA/IEC 62443, AWWA, and PLC Top 20 Secure Coding practices.

Tools: Wireshark, etcetera.

Trainings: OSHA 30 General Industry, etcetera.

Employer: Jacobs

Title: SR ICS OT Cybersecurity Engineer **Salary \$178,000/yr. full-time**

Start/End Dates: January 2019 – March 2020

Scope/Description: Providing end to end lifecycle specialized ICS OT and cyber security expertise for global multisector automation, control system, operational technology, SCADA, distributed control system, safety system and other process control systems for various critical infrastructure customers and partners. Providing technical ICS OT cyber SME customer services leadership and advocacy for the global ICS OT Cyber community. Briefly served as acting ICS OT Cyber Technical Director leading field services globally. Executed a wide range of ICS OT security services such as ICS OT security assessments, systems security engineering including device functionality testing as well as fly away incident response services. Continuing to contribute to ISA84, ISA/IEC 62443, and AWWA.

Tools: Office365 suite, Kali, VirtualBox, NetworkMiner, CSET, Wireshark, Nmap, Kepware, Waterfall, Owl, SHODAN, Grassmarlin, Ghidra, etcetera.

Trainings: SANS ICS 612

Employer: LEO Cyber Security

Title: VP of Global ICS Security Service Delivery **Salary: \$172,000/yr. full-time**

Start/End Dates: January 2018 – October 2018

Scope/Description: Leading global ICS security service delivery teams and projects implementing ICS focused security controls and standards, conducting penetration tests, vulnerability, threat and risk assessments, security testing during Factory and Site acceptance tests (FAT/SAT) and systems security engineering throughout lifecycle of ICS engineering projects. Leveraged native OS commands, open source tools and commercial tools for scanning, sniffing, functional feature analysis etcetera as needed. Creating innovative ideas such as “ICS Security Manager as a Service” and Security Practices and Recommended Guidelines for IEC 61131-3 PLC programming languages. Also continuing to be an active member of ISA99/IEC (62443), ISA84 and AWWA standards committee. Co-taught ICS security Red Team vs Blue Team training with ThreatGen.

Tools: Kali, Tenable Nessus, OpenVAS, VirtualBox, NetworkMiner, CSET, Wireshark, Nmap, Indegy (now Tenable OT), RF SDR tools, ELK, Security Onion, Trello, Google Office Suite, SHODAN, Grassmarlin, etcetera.

Trainings: PLC programming classes, ELK Master Class, Powershell, Python for Hackers, Security Tube and Pentester Academy courses, Arduino and RaspberryPi courses etcetera.

Employer: Fortress Information Security

Title: Director of OT Security Solutions **Salary: \$160,000/yr. full-time**

Start/End Dates: July 2017 – December 2017

Scope/Description: Led OT security services and operations to integrate Fortress products and services with existing infrastructures of critical infrastructure sector customers. Provided creditability for the Fortress OT products and services offerings, exposing Fortress leadership to organizations, events, authoritative sources, and points of contact to further improve and inform Fortress OT offerings to customers. Built additional service offerings such as security engineering assessment benchmarks, reports and teams for OT assets and operations. Responsible for OT product development and device testing, functional requirements and



capabilities and integration with third party partners and our customers. Provided leadership for all things OT to improve the capabilities of Fortress' platform and partner products. Developed project plans, implementation plans and operational templates to train and develop an OT operations staff. Conducted ICS security assessments, built ICS security roadmap POA&Ms and conducted product demo and network analysis of customer environments. Also continuing to be an active member of ISA99/IEC (62443), and ISA84 standards committees.

Tools: Cyberbit, Fortress Information Security, JIRA, Wireshark, Networkminer, etcetera.

Employer: Federal Energy Regulatory Commission (FERC) Office of Energy Infrastructure Security (OEIS)

Title: GS-2210-15 INFOSEC Specialist (TS/SCI, Q and PCII authorized User) **Salary:** \$136,000/yr. full-time

Start/End Dates: June 2016 – July 2017

Scope/Description: Provide cybersecurity expertise for industrial control systems (ICS) and information technology (IT) used by critical energy infrastructures such as hydro dams, bulk electric grid, liquefied natural gas terminals, oil, and gas pipelines. Educate Commission, infrastructure owners and operators, Congress and federal and state partners on cyber threats and mitigations for critical energy infrastructure. Champion or lead advanced visibility into ICS device, protocols, communications, and systems security to educate the Commission, infrastructure owners or operators and our federal, state, and local partners. Participated in Architecture Reviews and voluntary security advisory services for selected asset owners. Created ICS security best practices domains to be shared with our partners and with State Utility Commissions. Served as an ICS security SME on the interagency Smart Grid Task Force Group and supported collaboration with GridEx, SEPA, and SGIP as needed.

Trainings: Powershell, Python for Hackers, Security Tube and Pentester Academy courses, Arduino and RaspberryPi courses, UC Irvine Coursera Embedded Systems classes, etcetera.

Employer: Risk Mitigation Consulting (RMC)

Title: Cybersecurity Specialist IV (ICS) (Secret and interim TS) **Salary:** \$118,000/yr. full-time

Start/End Dates: June 2014 – June 2016

Scope/Description: Provided cybersecurity expertise on Mission Assurance Assessments, Energy Security Assessments and Operational Utility Technology Assessments of various critical infrastructure types and their industrial control systems for US Navy (USN) and US Marine Corps (USMC) bases around the US, Europe, Africa and the Middle East. This included but was not limited to assessing industrial control systems and critical mission systems for airfields and airports used by USN or USMC, electric substations, water and wastewater facilities and equipment, oil, gas and fuel facilities, advanced meter infrastructure (AMI), building control systems, satellite stations, fire, life safety and emergency operations center systems, land mobile radio (LMR) stations and chemical, biological, radiological, nuclear and explosive (CBRNE) detection systems or equipment. Assessments took an all threats all hazards approach through walk downs of equipment and operations areas, interviews of personnel, collection of documentation and when capable access to systems to review basic systems configurations etcetera. The purpose was to look for attack surfaces that could threaten to degrade mission critical operations or harm personnel. I also provided Information Systems Security Engineer and cybersecurity consulting expertise to ICS vendors such as Siemens and USMC bases to champion or lead the implementation of Risk Management Framework (RMF) security controls on ICS. My expertise also influenced business growth for my company as well as the advancement of ICS cybersecurity expertise, policies, templates, procedures and directives for ICS vendors and USMC. Supporting and collaborating with HQMC PPO, C4 CY, MCICOM, NAVFAC, NCIS, OPNAV N4 and USN/USMC AOR service components of COCOMs.

Tools: Office365 suite, XACTA, Archer, Wireshark, CSET, Grassmarlin, STIGs, STIGviewer, SHODAN, Kali, Siemens Apogee, Automated Logic Webctrl, etcetera.

Trainings: INL/ICS-CERT ICS 301, Antiterrorism awareness, SERE awareness, CISSP bootcamp, C|CISO bootcamp, John C. Maxwell 21 Irrefutable Laws of Leadership Mastermind, etcetera.



Employer: Key Concepts Knowledgebase

Title: Senior Cybersecurity Consultant (**Secret**) **Salary: \$95,000/yr. full-time**

Start/End Dates: October 2013 - June 2014

Scope/Description: Provided tier two and tier three cybersecurity analyst and incident response expertise to the US Patent and Trademark Office (USPTO) and Evolver Inc. within a 24/7/365 Network and Security Operations Center known as the CIO Command Center (C3). I helped to improve malware analysis and incident response capabilities of Evolver personnel and the USPTO.

Tools: Juniper, Fireeye MPS, Qradar, BMC Remedy, Maltego, Symantec etcetera.

Employer: Indigo IT

Title: Cybersecurity Consultant **Salary: \$80,000/yr. full-time**

Start/End Dates: October 2012 – October 2013

Scope/Description: I provided incident response, continuous monitoring and vulnerability management expertise and operations support to the Chief Information Security Officer (CISO) of the Federal Housing Finance Agency (FHFA) and his staff. Ran all scanning, monitoring, malware analysis and host-based security tools daily. I also provided advisory lessons learned support to the CISO of the National Credit Union Administration (NCUA) as he began to build out NCUA's cybersecurity program.

Tools: Tenable SC and Nessus, Rapid7 Nexpose, Qualys, Qradar, Sourcefire, Fireeye MAS, McAfee ePO, etcetera.

Trainings: EC-Council CEH v7

Employer: US Navy, Naval Supply Systems Command (NAVSUP) Business Systems Center (BSC)

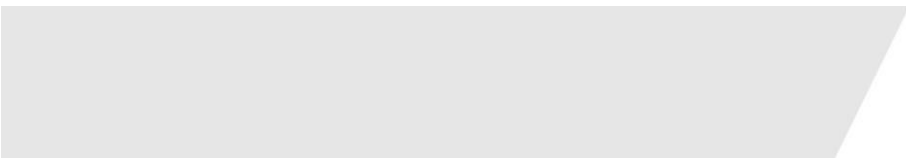
Title: GS-2210-11 INFOSEC and Systems Analyst (**Secret**) **Salary: \$65,000/yr. full-time**

Start/End Dates: July 2005 – October 2012

As an Information Assurance Officer/Information Systems Security Officer, I ensured the confidentiality, integrity and availability of assigned NAVSUP and US Navy enterprise systems. I ensured the systems obtained and maintained their Authority to Operate (ATO) under the Defense Information Assurance Certification & Accreditation (DIACAP) program by ensuring that technical and process security controls were implemented within systems and program management lifecycles. I also created and co-hosted configuration control boards with Program Managers and Contract Officers to ensure information assurance requirements remained within the system lifecycle. Additionally, I was a Host Based Security System (HBSS) security analyst supporting the team lead in ensuring the system was properly maintained for laptops, desktops, and servers within the command's legacy network and in accordance with Defense Department and US Navy security operations requirements.

As a systems analyst, I provided systems analysis, design, business process reengineering and continuous process improvement support for NAVSUP Enterprise implementation of SAP software through the US Navy Enterprise Resource Planning (ERP) project. I personally resolved over 600 hundred trouble tickets, identified and tested SAP defects, cleared over \$5 million in unmatched transactions for critical payment interfaces and led a Lean Six Sigma Greenbelt project to reduce command vehicle usage costs by up to 30% from the previous fiscal year.

As an IT Intern, I provided various levels of support for command special projects and assigned enterprise projects. Support included project management support, application development or programmer support and systems design or functional analyst support. A major project of note was my project management software expertise support for the Defense Property Accountability System (DPAS) which was the Department of Defense asset accountability system of record.



Tools: .Net 2005 suite, Windows XP, Windows 7, defense connect online (DCO), HBSS, eyeRetina, SAP ERP ECC 5.0, HEAT ticket system, MS Access, MS Project, MS Visio, Primavera, NAVSISA DIACAP Status Tracker, etcetera.

Trainings: Information Assurance trainings, SANS IPv6, DON Lean Six Sigma, Federal Appropriations, SAP PLM, McAfee HBSS, .Net 2005 suite bootcamp, Security+ bootcamp, etcetera.

Employer: First Health Services Corp-Pace Operations

Title: Clerk, Manufacturer Rebate Asst.

Start/End Dates: May 2004 – August 2004

Scope/Description: Provided office administrative assistance such as mailing and filing. Also provided operations management assistance including verifying, updating, and maintaining data integrity, data confidentiality and access control of a Windows DOS database. Contacting medical professionals and manufacturers to verify paper-based information and aid operations managers in migrating from a paper-based file cabinet system to Windows DOS electronic records database. Confidentiality, Integrity and Availability of manufacturer and medical patient data was paramount to company rebate manufacturing services operations.

Tools: MS Windows DOS, Floppy Disk, etcetera.