**Alvaro A. Sanchez Almanzar Clearance:** PublicTrust (IRS)

**Level:** Lead Engineer  **Residence:** Clarksburg, Md

**Email:** [alvaro1688@gmail.com](mailto:alvaro1688@gmail.com) **Willing to relocate:** No

**Cell:** (301)8205977 **% Willing to Travel:** 0%

**Last update:** 8/19/2025

# EXPERIENCE SUMMARY

Dedicated Risk Management and Cyber Security Analyst with over 7 years of hands-on experience in ensuring robust security postures for complex systems within corporate environments. Proficient in leveraging Tenable Security Center, Qualys, Nessus Professional, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and Center for Internet Security (CIS) Benchmarks for vulnerability assessments and compliance scans. Demonstrated expertise in navigating the Federal Information Security Modernization Act (FISMA) lifecycle, National Institute of Standards and Technology (NIST) 800-53 controls, and the Federal Risk and Authorization Management Program (FedRAMP) security packages. Adept at liaising with cross-functional teams to ensure timely remediation of security vulnerabilities and seamless cloud transitions. Proven leader in developing and maintaining comprehensive system security plans and POA&M strategies. Python and .Net entry level developer.

Detail-oriented and results-driven PowerBI Data Analyst with 3 years of experience in collecting, transforming, and visualizing data to create dynamic dashboards and reports. Expertise in developing interactive PowerBI reports, performing data modeling, and collaborating with stakeholders to deliver data-driven insights. Skilled in optimizing data models, enhancing reporting performance, and translating complex datasets into user-friendly business intelligence solutions.

## **CERTIFICATIONS**

ISC2 CC  
CompTIA Security+

CompTIA CASP+

Azure AZ-900

SAFe Agilist 6.0

## **EDUCATION**

A.A.S Cyber Security, Montgomery College, 2018

## **SUMMARY OF SKILLS, TOOLS, AND TECHNOLOGIES**

### **Coding Languages:** Python, C#, HTML & CSS, JavaScript (Learning), Terraform (IaC) **CyberSecurity Tools:** Nessus (Tenable Security Center), Qualys, ServiceNow, Jira, Rcats, **Operating Systems:** Linux (5 yrs), Windows (15yrs), Mac OS (15yrs)

### **Data Analysis:** PowerBI Data visualization & Dashboard creation (2yrs+)

# EXPERIENCE DETAILS

## **Booz Allen Hamilton (NIH Project) & (IRS Project-IRS Cleared)**

*October 2022 – April 2025*

Senior Cybersecurity Vulnerability Engineer

* Led the implementation of the Risk Management Framework (RMF) process to support the system's journey to Authorization to Operate (ATO), ensuring compliance with NIST SP 800-53 rev.5 and other federal cybersecurity requirements.
* Collaborated with system owners, Information System Security Managers (ISSMs), and Authorizing Officials (AOs) to develop and review security documentation, including System Security Plans (SSPs), FIPs-199 Security Categorization, Business Impact Analysis (BIA), and other core documents.
* Assisted with the development of contingency and disaster recovery plans, ensuring alignment with security and risk management policies.
* Provided subject matter expertise on RMF processes to internal teams, ensuring a clear understanding of requirements and supporting compliance efforts.
* Contributed to the creation of security documentation for ATO submission, including security categorization, risk assessments, and compliance evidence.
* Collaborated with cross-functional teams to prioritize ATO deliverables.
* Worked with the CASO team on updating and creating Cloud security documents and following up their step-by-step process.
* Led vulnerability assessment programs, by identifying, and analyzing security vulnerabilities across the organization's infrastructure.
* Developed and implemented comprehensive vulnerability management strategies, ensuring timely detection and remediation of security risks.
* Collaborated with cross-functional teams to prioritize and mitigate critical vulnerabilities, reducing the organization's overall security risk posture.
* Conducted regular vulnerability assessments to proactively identify weaknesses and recommend security enhancements.
* Implemented and managed security tools and technologies to automate vulnerability scanning and remediation processes, resulting in increased efficiency and reduced time to resolution.
* Mentored and trained junior team members, fostering a culture of continuous learning and skill development.
* Prepared and presented reports to executive leadership, providing insights into the organization's security posture, and recommending proactive measures.
* Stayed abreast of the latest cybersecurity trends, emerging threats, and vulnerability management best practices to keep the organization's security posture ahead of potential risks.
* Created, tracked, and managed system Plans of Action and Milestones (POA&Ms).
* Data Collection & Preparation: Gather data from various sources (e.g., databases, spreadsheets, cloud services) and preprocess it to ensure accuracy and consistency for reporting.
* Data Modeling: Build and optimize data models in PowerBI, creating efficient relationships between datasets and implementing calculated columns and measures using DAX to enhance reporting capabilities.
* Dashboard & Report Creation: Design and develop interactive PowerBI dashboards and reports that provide actionable insights to stakeholders, incorporating a variety of charts, tables, and visuals.
* Collaboration with Stakeholders: Work closely with business users, including executives and managers, to understand reporting requirements, ensuring dashboards meet their needs and provide meaningful data.
* Quality Assurance: Validate the accuracy and consistency of data in dashboards, ensuring real-time or up-to-date information. Troubleshoot and resolve any issues related to data sources or report functionality.

## **WhiteHat Auditors**

*December 2021 to October 2022*

Senior Cybersecurity Engineer and Information Assurance Specialist

**(Summarized)**

* This role involved leading the vulnerability management program, overseeing the full lifecycle from identification to remediation. Responsibilities included preparing documentation based on customer information using accepted guidelines like the Risk Management Framework (RMF) and working with Information System Security Officers (ISSOs) and the Authorizing Official (AO) to support FISMA systems through the Security Assessment & Authorization (SA&A) lifecycle.

• The position also involved preparing Security Test and Evaluation Plans, providing certification and accreditation support, and conducting risk and vulnerability assessments. Duties included analyzing policies against federal regulations, developing and updating system security and contingency plans, recommending security improvements, scanning systems for compliance, and performing vulnerability assessments.

• The role also required communication with auditors, creation and management of Plans of Action and Milestones (POA&Ms) and conducting configuration compliance checks against standards like DISA STIGs and CIS Benchmarks.

## **The Department of Energy**

*12/2019 – 12/2021*

Federal Employee

Germantown Md

Information System Security Officer (ISSO)

**(Summarized)**

* The role involves reviewing business system missions and objectives, collaborating with system owners and the Information System Security Manager (ISSM) to ensure compliance with NIST, the Office of the Chief Information Officer policies, and the risk-based cybersecurity program for CFO-managed applications. Responsibilities include assisting with drafting system security plans (SSP), system categorization, business impact analysis, contingency plans, and obtaining ISSM approval.

• The position also entails developing and maintaining security authorization package documentation, including security plans, disaster recovery plans, privacy impact assessments, and Plans of Actions and Milestones (POAMs), and ensuring timely updates to system security plans. The individual will coordinate annual assessments and accreditations, track Authorization to Operate (ATO) dates, review risk logs, and provide recommendations for resolution.

• Other duties include supporting privileged and service account reviews, analyzing vulnerability scans, offering mitigation strategies, tracking vulnerabilities, and staying informed on emerging threats, offering solutions, and conducting reconnaissance activities for FISMA systems.

## **Oasis Systems**

***(****08/2018 – 12/2019)*  
Federal Contractor

Rockville, MD

Information Assurance & Vulnerability Specialist

**(Summarized)**

• The role involves preparing documentation based on customer information using guidelines like the Risk Management Framework (RMF), collaborating with Information System Security Officers (ISSOs) and Authorizing Officials (AOs) to support FISMA systems through the Security Assessment & Authorization (SA&A) lifecycle.

• Responsibilities include creating Security Test and Evaluation Plans, assisting with certification and accreditation, developing security and contingency plans, conducting risk and vulnerability assessments, and analyzing policies for compliance with federal regulations.

• The position also involves recommending system enhancements to address security deficiencies, scanning for compliance, and performing vulnerability assessments, configuration compliance checks, and risk mitigation strategies using standards such as DISA STIGs and CIS Benchmarks.