**Alvaro A. Sanchez Almanzar**

**Email:** [alvaro1688@gmail.com](mailto:alvaro1688@gmail.com)

**Cell:** 301-820-5977

**Last update:** 5/5/2025

# EXPERIENCE SUMMARY

Experienced Risk Management and Cybersecurity Analyst with 7+ years in securing corporate systems. Skilled in vulnerability assessments using Tenable, Qualys, Nessus, and compliance with DISA STIGs and CIS Benchmarks. Deep knowledge of **FISMA**, **NIST 800-53**, and **FedRAMP**. Strong track record in system security planning (**SSP**), **POA&M** development, and cross-functional collaboration. Also, a junior-level Python, HTML & CSS, and .NET / C# developer. Additionally, a results-driven **PowerBI** Data Analyst with 2 years of experience in data visualization, dashboard development, and delivering actionable business insights.

## **CERTIFICATIONS**

✔️ ISC2 CC  
✔️CompTIA Security+

✔️CompTIA CASP+

✔️Azure AZ-900

## **EDUCATION**

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

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

### Coding Languages

Python, C#, HTML (Learning), CSS (Learning), JavaScript (Learning), Terraform (Training Completed)

## Nessus (Tenable Security Center**)**

Automated & Manual Scans (7 yrs)

### Operating Systems

Linux (5 yrs), Windows (15yrs), Mac OS (15yrs)

### PowerBI

Data visualization & Dashboard creation (2yrs)

# EXPERIENCE DETAILS

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

*October 2022 – Present*

Senior Cybersecurity Vulnerability Engineer

* Led the end-to-end implementation of the Risk Management Framework (**RMF**) process to achieve Authorization to Operate (**ATO**), ensuring compliance with NIST SP 800-53Rev.5 and federal cybersecurity standards.
* Collaborated with system owners, ISSMs, and Authorizing Officials to develop core security documentation including **SSPs, FIPS-199, BIAs, and POA&Ms**. Played a key role in cloud security documentation with CASO and guided cross-functional teams through ATO deliverables.
* Organized vulnerability assessment initiatives, driving enterprise-wide risk reduction through automation, prioritized remediation, and strategic collaboration. Designed and executed a comprehensive vulnerability management strategy, significantly reducing resolution times and improving infrastructure resilience.
* Delivered data-driven insights through advanced **PowerBI** dashboards and **Excel** reporting. Built optimized data models using **DAX**, integrated multiple data sources, and collaborated with stakeholders to deliver impactful visualizations for executive decision-making. Trained users, maintained dashboard performance, and ensured high data integrity across reporting pipelines.

## **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 (**BIA**), contingency plans (**CP**), 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 position also entails coordinating 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.