Last updated in Mar 2025

Justin Johnson, PMP, CISSP, MBA

Atlanta, GA mail@justinmjohnson.com (850) 691-9708 www.justinmjohnson.com
imjustinjohnson justin-m-johnson

Cybersecurity Analyst Lead

Cybersecurity Analyst Lead with over 10 years of comprehensive experience driving cybersecurity initiatives and IT governance projects. Demonstrated expertise in leading cross-functional teams and managing complex projects to enhance compliance, risk management, and security posture. Proven ability to implement industry best practices, including Zero Trust architecture and NIST Risk Management Framework (RMF), while optimizing cloud security, vulnerability management, and governance frameworks. Adept at balancing technical proficiency with project leadership to deliver timely, high-impact results aligned with organizational goals.

Education

MBA **Western Governors University**, MBA - IT Management — Oct 2024 – Apr 2025
- 4.0 GPA
- Masters of Business Administration-IT Management

B.Sc **Colorado State University-Global Campus**, Cyber Security — Aug 2016 – May 2018
- 4.0 GPA
- Magna Cum Laude

B.Sc **Florida State University**, Criminology — Aug 2007 – May 2011
- 3.7 GPA

Experience

Cybersecurity Analyst Lead, Alpha Omega – Atlanta, GA (Remote) — July 2025 – present

- As a Project Manager and Cybersecurity Analyst Lead/Systems Security Steward Lead at Alpha Omega, following its acquisition of SeKON Enterprise, I have successfully navigated organizational change while expanding my leadership capacity and driving vital cybersecurity projects supporting the CDC's public health mission.
- Spearhead comprehensive project management efforts within cybersecurity initiatives, overseeing project planning, resource coordination, timeline management, and performance tracking to ensure timely, quality delivery aligned with strategic objectives.
- Lead and mentor a team of Cybersecurity Analysts and Systems Security Stewards, fostering collaboration and professional growth to maintain focus on enhancing CDC's information systems security posture amid digital transformation.
- Direct and coordinate Authorization & Accreditation (A&A) workflows based on the NIST SP 800-37 Risk Management Framework (RMF), meticulously managing project documentation, schedules, and stakeholder communications.
- Champion vulnerability management and compliance assessment programs, orchestrating workflows to meet federal standards and CDC security mandates.- Establish and disseminate best practices in cybersecurity monitoring and risk mitigation, driving process improvements that support CDC's evolving security strategy.
- Serve as the primary liaison with internal stakeholders, providing clear updates on project progression, risk identification, and mitigation strategies to ensure informed decision-making and accountability.
- Chair Configuration Control Board (CCB) activities, facilitating key project meetings to manage cybersecurity-related changes and ensure configuration items are tracked and implemented.

Information Systems Auditor SME, SeKON – Atlanta, GA (Remote) Oct 2024 – July 2025

- As an Information Systems Analyst SME/Systems Security Steward Lead, I support the CDC's mission to protect public health through innovative IT solutions and robust cybersecurity measures. Working with SeKON Enterprise, Inc., I contribute to the security, integrity, and compliance of the CDC's information systems while supporting the agency's digital transformation efforts.
- Leading a team of Information Systems Analysts/Systems Security Stewards in supporting the CDC's mission to protect public health through innovative IT solutions and robust cybersecurity measures
- Execute Authorization & Accreditation (A&A) processes within the NIST SP 800-37 Risk Management Framework (RMF).
- Evaluate information systems' security control compliance with federal requirements and CDC's monitoring strategy.
- Ensure system operations align with approved security authorization packages.
- Vulnerability Management
- Conduct annual assessments to ensure compliance with CDC standards.
- Participate in Configuration Control Board (CCB) activities to manage cybersecurity-relevant configurations.
- Provide expert guidance on cybersecurity best practices and CDC's monitoring strategy.
- Communicate effectively with stakeholders to track and report on information system monitoring efforts.

Information Systems Engineer Lead, SeKON – Atlanta, GA (Remote) Oct 2022 – Oct 2024

- Reviewed the guidance from CISA and DISA and offered recommendations to our current Cyber team members on how to effectively implement best practices based on that guidance.
- Analyzed Executive Orders (EO), Office of Management and Budget (OMB) policies, and other relevant guidelines to offer additional instructions and insights to team members. This included topics such as Zero Trust (NIST 800-207) and the changes introduced in NIST RMF Revision 5.
- Received Cyberspace Tasking Orders from JFHQ-DODIN and offered guidance to system engineers and administrators on addressing remediation tasks and meeting the specified deliverables.
- Received multiple recognitions from Government and Corporate Leadership for delivering outstanding results in a timely and efficient manner.
- Implemented Cybersecurity Dashboards integration with several Programs/Systems of Record
- Developed Splunk Dashboards to be used as a SIEM tool to monitor system logs and events, metrics, and NIST 800-53 Control Families
- Implemented Automated Vulnerability Scanning capabilities which were directly/automatically fed into eMASS.
- Reviewed Quarterly STIGs and SCAPs for each Information System to Ensure Compliance was met.

Information Systems Engineer, SeKON – Atlanta, GA (Remote) Aug 2020 – Oct 2022

- Cybersecurity leader with a proven track record in elevating government systems to full ATO certification. Successfully spearheaded the transition of multiple Systems of Record from ATO-C to ATO status, showcasing expertise in security compliance and stakeholder management. Adept at devising efficient strategies to meet stringent government regulations while fostering seamless collaboration between technical teams and government stakeholders.
- Implemented DISA's Continuous Monitoring and Risk Scoring (CMRS) system's API to eMASS for various Information Systems, utilizing ACAS Security Center for integration with eMASS.
- Conducted weekly ACAS scans, supported ISSOs during Quarterly and Annual Security Reviews, selecting appropriate STIGs/SRGs and reviewing STIG checklists.Ensured system security requirements, tools, and architecture compliance for various systems.
- Actively participated in Configuration Management, Change Requests, and POA&Ms throughout the RMF Lifecycle, focusing on steps 2-4 and 7.
- Authored Standard Operating Procedures (SOPs) for Cyber Security and Information Systems Security Engineering teams.

Information Systems Security Officer, Georgia Tech Research Institute – Atlanta, GA — Nov 2018 – Aug 2020

- Implemented the Risk Management Framework (RMF), NIST SP 800-37, JSIG, and other relevant compliance documents.
- Developed Security Documentation for Information Systems, including SCTM, SSP/SAP, Contingency Plans, RAR, Continuous Monitoring, and POAM, while maintaining system design throughout the lifecycle.
- Conducted weekly vulnerability scans using Nessus and Splunk, with monthly patching of Nessus scanners.
- Delivered weekly and annual cyber-security training for technical and non-technical personnel.

IT Technician, Mount Vernon Towers – Atlanta, GA — July 2018 – Nov 2018

- Redesigned company network to enhance data efficiency and reduce costs by integrating external services.
- Established testing and hardening practices for network and physical security.
- Assisted residents and employees with daily IT issues and new technologies.
- Managed wireless and wired networks, VPN, and IP/POT telephones.

Corporal, Field Services Division, Bay County Sheriff's Office – Panama City, FL — July 2013 – July 2018

- Supervised and led multiple patrol deputies.

Current Certifications

Project Management Professional, PMI

ISC(2), CISSP

Microsoft, Azure Fundamentals

Microsoft, Office 365 Fundamentals

Microsoft, Security Compliance and Identity Fundamentals

CompTIA, Security+

CompTIA, Network+

CompTIA, A+

Projects

Hybrid Cloud Homelab — github.com/justinmjohnson/homelab

- Currently designing and implementing a hybrid cloud homelab as a testing environment for Proof of Concept (PoC) ideas.
- Utilizes several logging and monitoring solutions such as Splunk and Wazuh.
- CI/CD Pipelines for automation with Github Actions.
- Integrated security tools for streamline development and testing processes.

Technologies

Languages: Python, Powershell, Bash, Git

Technologies: Cloud (AWS, Azure, GCP, Oracle) VMware, KVM, Hyper-V

Tools: Ansible, Terraform, Splunk, Wazuh, Nessus, VMware, AWS, Azure, Docker, Splunk, ELK, Nessus

Regulatory Compliance: NIST 800-37/800-53/800-171, Zero Trust (800-207), HIPAA, JSIG, NIST Cybersecurity Framework