

Jason Carter

Virginia Beach, VA | jcart098@odu.edu | linkedin.com/in/jason-carter-0202b9228 | sites.wp.odu.edu/jasoncarter

Cybersecurity student at Old Dominion University and CompTIA Security+ holder specializing in cybersecurity compliance, with hands-on CMMC Level 1 and Level 2 experience through an active internship at RFK Solutionz. Backed by practical offensive security skills in vulnerability assessment and penetration testing. Seeking a compliance or GRC role where documentation rigor and technical fluency both matter.

EDUCATION

Old Dominion University, Norfolk, VA

Expected December 2026

B.S. in Cybersecurity | GPA: 3.7

Relevant coursework: Linux Systems for Cybersecurity, Cybersecurity Techniques & Operations, Cryptography, Cybersecurity & the Social Sciences

Tidewater Community College, Virginia Beach, VA

December 2024

A.S. in Cyber Security

CERTIFICATIONS

CompTIA Security+

April 2023

EXPERIENCE

Cybersecurity Intern, RFK Solutionz

August 2026 – Present

Hands-on IT deployment and cybersecurity compliance (ODU CYSE 368)

- Built structured CMMC Level 1 and Level 2 compliance documentation covering scoping boundaries, ESP and cloud rules, domain requirements, and a six-phase action plan.
- Assessed end-of-life network hardware (Cisco 3845 router) against CMMC requirements and researched compliant upgrade paths.
- Co-developed an offensive security presentation and CTF challenge; performed privilege escalation testing.
- Deployed hardware and configured workstations, including operating system setup.
- Planned 10 interactive, game-based activities across two themed days for a Cyber Academy serving about 50 students.

Pool Gate Guard, AAA Pool Services, Virginia Beach, VA

July 2021 – September 2022

- Trained new staff on company policies and procedures.
- Monitored guests to identify safety concerns and enforce rules; maintained sign-in logs to support contact tracing.

TECHNICAL SKILLS

Tools: Nmap, Metasploit, Burp Suite, Wireshark, Nikto, Hashcat, John the Ripper

Areas: CMMC Level 1 and Level 2 compliance (scoping, gap assessment, documentation); vulnerability assessment and penetration testing; Linux administration and shell scripting; networking and subnetting; applied cryptography (ECC, AES, RSA)