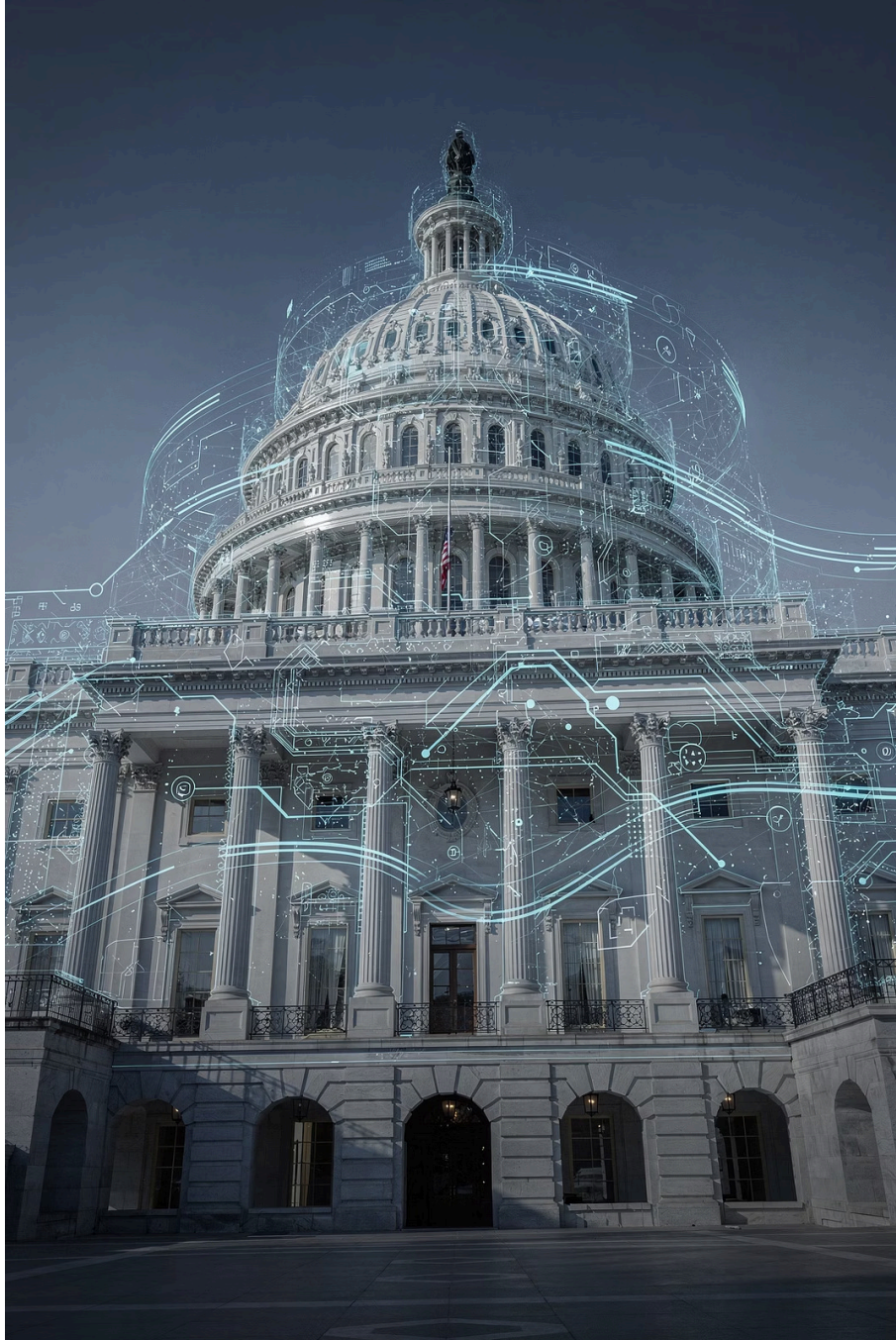
DC Cybersecurity Workforce: What the Data Actually Shows

Understanding the real landscape of cybersecurity job openings and talent gaps in the Washington, D.C. metropolitan area requires looking beyond headlines. This presentation examines current job market data, unfilled positions, and what we can reliably measure about one of America's most cybersecurity-intensive regions.

We'll explore active job postings, regional talent shortages, salary expectations, and the challenges in quantifying an ever-shifting workforce landscape where federal agencies and contractors drive unprecedented demand for security professionals.



CURRENT MARKET

Security Operations & Analyst Job Openings in DC

The Washington, D.C. and Baltimore metropolitan area shows substantial demand for security professionals, with thousands of active listings across major job boards. These numbers represent a snapshot of publicly posted positions, though many federal and clearance-required roles remain unlisted on aggregated platforms.

SOC Analyst Roles

Approximately **811 Security Operations Center (SOC) Analyst positions** currently listed in the Washington, DC area, spanning junior through specialized roles across various security domains.

Cyber Security Analysts

Over **2,000+ Cyber Security Analyst and Information Security Analyst jobs** posted across the broader DC-Baltimore regional area on platforms like LinkedIn.

These counts fluctuate weekly based on employer budgets, seasonal hiring patterns, and posting practices. The actual demand is likely higher since many government and contractor positions aren't publicly advertised.

TALENT GAP ANALYSIS

The Persistent Cybersecurity Talent Shortage

While exact annual counts of unfilled cybersecurity positions in D.C. don't exist in official statistics, regional workforce research reveals a significant and persistent gap between employer demand and available qualified talent.

Regional Shortage Data

The Maryland and DC region experienced an estimated 6,500 cybersecurity positions unfilled during just a two-month period from December 2023 to January 2024. This shortage stems from insufficient supply of workers with the necessary skills and clearances.

Perhaps most striking: only about **33% of cybersecurity needs** in the Maryland/DC region are currently met by available talent, meaning two-thirds of employer demand goes unmet.

> "Employer demand outstrips supply such that only about 33% of cybersecurity needs in the Maryland/DC region are met by available talent."

NATIONAL CONTEXT

Understanding DC's Workforce Gap Through National Trends

The Washington area's cybersecurity workforce challenges don't exist in isolation. As a hub for federal agencies, defense contractors, and heavily regulated industries, the region reflects and amplifies national workforce trends. Understanding the broader U.S. talent shortage provides essential context for local hiring difficulties.

466K+

National Shortfall

Estimated gap between current cybersecurity jobs and qualified professionals across the United States

100K+

Active U.S. Postings

Hundreds of thousands of cybersecurity positions advertised nationally with insufficient candidates to fill them

According to CyberSeek and CompTIA analysis, the national cybersecurity skills shortage persists despite some hiring stabilization. This widespread gap directly impacts the DC region, where competition for cleared professionals with specialized skills remains intense.

What This Means for Job Seekers in DC

Active Job Market

Right now, approximately **800+ SOC Analyst roles** and **2,000+ security analyst positions** are actively recruiting in the Washington DC metro area. These snapshot figures from recent job board data represent immediate opportunities across various security specializations.

Chronic Demand

Regional research indicates **thousands of cybersecurity roles remain unfilled** due to a shortage of qualified candidates. The estimate of 6,500 unfilled positions in a short Maryland/DC period signals ongoing, structural industry demand rather than temporary fluctuation.

Competitive Advantage

The national cybersecurity field faces a significant workforce gap, meaning employers want more qualified workers than are currently available. Even when postings show moderate numbers, underlying demand remains robust for skilled professionals.

MEASUREMENT CHALLENGES

Why Precise "Annual Unfilled Job" Numbers Don't Exist

There isn't a single official tally for "how many cybersecurity jobs go unfilled each year in DC" due to several structural factors that make precise measurement challenging:

- **Non-public sector roles:** Many government and contractor positions aren't published on open job boards due to security and clearance requirements
- **Seasonal and confidential hiring:** Federal and contractor recruitment is often clearance-dependent, budget-driven, and confidential in nature
- **Aggregation limitations:** Workforce reporting agencies compile data quarterly or annually at state/national levels, not as metro-specific daily counts
- **Dynamic market:** Postings, hiring freezes, and budget allocations shift constantly based on political and economic factors

DC Cybersecurity Workforce: Summary Overview

Category	Approximate Count	Source
SOC Analyst job postings (DC area)	~811+ current listings	LinkedIn
Cyber/Information Security Analyst listings	~2,000+ current listings	LinkedIn
Regional unfilled positions (recent short period)	~6,500+ unmet demand	TEDCO Maryland
National cybersecurity workforce gap	466,000+ supply shortfall	CyberSeek/PR Newswire

This data snapshot illustrates both the immediate opportunities available to job seekers and the broader structural challenges facing the cybersecurity workforce in the nation's capital region.

$ COMPENSATION ANALYSIS

Mapping Cybersecurity Jobs to DC-Area Salaries

Understanding compensation is critical for career planning. The following sections break down typical salary ranges for common cybersecurity and audit job titles in the Washington, DC area, based on recent market data from multiple sources including Indeed, Salary.com, Glassdoor, and specialized compensation platforms.

These figures reflect the DC market's premium over national averages, driven by high cost of living, intense competition for cleared professionals, and the concentration of federal agencies and contractors willing to pay top dollar for cybersecurity talent.

Security Operations

SOC Analysts and Cybersecurity Analysts form the frontline defense, with salaries ranging from entry-level to senior specialist positions

Audit & Compliance

IT Auditors and Systems Auditors ensure controls and compliance, with CISA certification commanding premium compensation

Governance & Risk

GRC Analysts manage risk frameworks and compliance programs, earning competitive salaries for their strategic expertise

SECURITY OPERATIONS

Security Operations & Analyst Role Compensation

Security operations professionals—from SOC analysts to cybersecurity analysts—represent the largest segment of DC's cybersecurity workforce. Compensation varies significantly based on experience level, certifications, and specialized skills.

Job Title	Typical Salary Range (DC)	Key Notes
SOC Analyst	~$85,000 – $115,000+/yr (avg ~$115K)	Entry to mid-level; certs boost pay
Cybersecurity Analyst	~$105,000 – $140,000+/yr (avg ~$116K)	Senior roles exceed this range
Senior Cybersecurity Analyst	~$136,000 – $160,000/yr	Advanced responsibilities
Entry-Level Analyst (0-2 yrs)	~$82,500 – $100,000/yr	New grads/cert holders

Sources: Indeed, Salary.com, Levels.fyi

AUDIT & RISK

IT Audit, Risk & GRC Role Compensation

Information Systems & IT Auditor Roles

IT auditors evaluate security controls, assess compliance, and identify risks. The CISA certification significantly enhances earning potential in these roles.

Role Level	Salary Range
Information Systems Auditor	$78,000 – $105,000/yr
IT Auditor (mid-level)	$100,000 – $145,000/yr
Senior IT Auditor	$121,000 – $171,000/yr

Governance, Risk & Compliance

GRC professionals manage enterprise risk, ensure regulatory compliance, and develop security frameworks:

- **GRC Analyst:** ~$96,000 – $147,000/yr (avg ~$118K)
- **Senior GRC/Risk Roles:** ~$125,000+ with bonuses common

Sources: Salary.com, Indeed, ZipRecruiter, Robert Half, Glassdoor

Federal & National Compensation Benchmarks

National Median (BLS)

The Bureau of Labor Statistics reports a **national median salary of $124,910/year** for Information Security Analysts across all markets. This serves as a useful baseline for comparison.

DC Premium

The Washington DC metropolitan area typically pays 15-25% above the national median due to cost of living, clearance requirements, and intense competition for talent among federal agencies and contractors.

Federal Pay Scales

Government positions follow GS pay scales, with cybersecurity roles typically ranging from **GS-11 to GS-15** ($75K-$160K+ with locality adjustments), plus contractor roles often offering higher compensation.

CERTIFICATIONS

How Certifications Impact Your Earning Potential

Industry certifications serve as powerful salary accelerators in the DC market, often determining entry qualifications and advancement opportunities. Here's how key certifications influence compensation:

Network+ & Security+

Foundation certifications that open doors to entry and junior roles, typically placing professionals in the **$80K – $110K range** early in their careers

CySA+ (Cybersecurity Analyst)

Advances analysts toward stronger SOC and threat detection roles, with experienced professionals averaging **above $100K** and climbing

CISA (Certified Information Systems Auditor)

Highly valuable for audit, GRC, and compliance positions; mid-to-senior auditors often **exceed $100K**, with senior roles reaching **$120K – $170K+**

Exact compensation varies by employer type, clearance requirements, years of experience, and the specific scope of responsibilities. Combining multiple certifications with hands-on experience yields the strongest salary outcomes.

DC Metro Salary Snapshot: Entry to Senior Levels

This comprehensive snapshot shows typical salary progression across key cybersecurity roles in the DC metropolitan area. Understanding these ranges helps job seekers set realistic expectations and plan career advancement strategies.

Category	Entry/Junior	Mid Level	Senior/Specialized
SOC Analyst	~$85K – $100K	~$100K – $115K	~$115K+
Cybersecurity Analyst	~$90K – $110K	~$110K – $140K	~$140K+
IT Auditor/Systems Auditor	~$78K – $100K	~$100K – $120K	~$120K – $170K+
GRC/Risk Analyst	~$95K – $110K	~$110K – $130K	~$130K+

Career progression typically involves 2-4 years at each level, though exceptional performers with strong certifications and clearances can advance more rapidly in the competitive DC market.

Key Compensation Takeaways for DC Job Seekers

Strong Entry Salaries

Entry-level roles for professionals building experience typically start in the **mid-$80Ks to low-$100Ks range**, significantly above national averages and reflecting DC's competitive market dynamics.

Six-Figure Mid-Career

Mid-career analysts and auditors with relevant certifications (Security+, CySA+, CISA) consistently see salaries **above $100,000**, with many positions offering performance bonuses and clearance premiums.

Premium Senior Roles

Senior or specialized positions—such as senior IT auditors, principal analysts, or GRC leaders—can approach **$150K+ in the DC area**, with some roles at major contractors exceeding $200K total compensation.

The combination of persistent talent shortages, federal agency demand, and high cost of living creates a seller's market for qualified cybersecurity professionals in the Washington, D.C. region.

Your Path Forward in DC Cybersecurity

The Washington, D.C. cybersecurity job market presents exceptional opportunities for professionals at all career stages. With thousands of positions available, persistent talent gaps, and competitive compensation, the region offers a robust foundation for building a successful security career.

Build Your Foundation

Start with fundamental certifications (Network+, Security+) and entry-level roles in the $80K-$100K range

Advance Your Skills

Pursue specialized certifications (CySA+, CISA) and gain hands-on experience to reach six-figure compensation

Lead & Specialize

Develop expertise in high-demand areas and move into senior roles earning $150K+ with leadership responsibilities

> With over 2,000 active postings, 6,500+ unfilled regional positions, and salaries well above national averages, the DC area remains one of America's premier markets for cybersecurity professionals.

Whether you're entering the field or advancing your career, the data clearly shows: DC needs your skills, and employers are willing to compete for your talent.