



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

THE ULTIMATE GOVCON SURVIVAL GUIDE 2026 EDITION

Six standalone guides. One comprehensive resource.

UPDATED MAY 2026 • VERSION 2.0

Everything we wish someone had handed us when we entered the cleared workforce. **Fact-checked against current policy** (Trusted Workforce 2.0, DoDM 8140.03, FY 2026 DCSA rates), reorganized for clarity, and built to be a baseline reference — not a substitute for your FSO, sponsoring agency, or qualified counsel.

THE SIX GUIDES INSIDE

- | | | |
|-----------|--|-------------|
| 01 | Security Clearances — A Complete Guide
Clearance levels, investigation tiers, the process today, public trust vs clearance, maintaining your standing under Continuous Vetting. | Pages 2–5 |
| 02 | DoD Cyber Workforce — DCWF & 8140
What changed when 8570 was cancelled, the DCWF framework, role-based qualifications, and the certifications that still drive cleared cyber hiring. | Pages 6–9 |
| 03 | GovCon Foundations — A Starter Guide
How GovCon works, the contract lifecycle, job stability realities, breaking in without experience, and clearance sponsorship paths. | Pages 10–13 |
| 04 | Compensation Playbook
2025–2026 cleared salary data, pay structures and schedules, shift differentials, market value, and the negotiation playbook. | Pages 14–17 |
| 05 | The Career Toolkit
Resume fundamentals, content that converts, certifications and tailoring, working with recruiters, red flags, and the Tier One 10. | Pages 18–21 |
| 06 | Cleared Pro Resources
Curated library of job boards, training, clearance tools, compensation tools, networking, transition programs, mental health, and news sources. | Pages 22–25 |



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

SECURITY CLEARANCES

A Complete Guide for Federal Candidates & Cleared Professionals

UPDATED MAY 2026 • VERSION 2.0

Security clearances are the entry pass to federal classified work — but the rules, systems, and timelines have changed substantially under **Trusted Workforce 2.0**. This guide is a plain-English baseline covering clearance levels, investigation tiers, the application and adjudication process, public trust positions, and how continuous vetting is reshaping the way clearances are maintained.

WHAT'S NEW IN 2026

- **Trusted Workforce 2.0 (TW 2.0)** Periodic reinvestigations are being eliminated. Continuous Vetting (CV) — automated, ongoing record checks — is the new standard. The old “TS every 5 / Secret every 10 / Confidential every 15” cycle no longer drives reinvestigations.
- **DISS to NBIS Transition** The National Background Investigation Services (NBIS) is gradually replacing DISS, e-QIP, and JPAS as the federal end-to-end vetting system. eApp has already replaced e-QIP for the SF-86. Full NBIS deployment is currently projected by FY2028.
- **Investigation Tiers Are Consolidating** DCSA is transitioning from the legacy 5-tier framework (T1–T5) to a streamlined 3-tier model (Low / Moderate / High). Both currently coexist; legacy products are being phased out over the next several years.
- **Continuous Vetting Enrollment** DoD completed the transition to CV in 2021. Federal agencies were required to enroll Non-Sensitive Public Trust personnel into CV by September 30, 2025.

CONTENTS

01	Clearance Levels & Designations	Page 2
02	Investigation Tiers (Legacy & Current)	Page 2
03	The Clearance Process Today	Page 3
04	Public Trust vs. National Security Clearance	Page 3
05	Maintaining Your Standing Under Continuous Vetting	Page 4
06	Key Systems & Agencies	Page 4
07	Reciprocity & Portability	Page 4

01 • CLEARANCE LEVELS & DESIGNATIONS

A security clearance authorizes access to classified information based on the potential damage to national security from unauthorized disclosure. The three core clearance levels are set by Executive Order 13526; additional designations layer on top for compartmented or special-access information.

National Security Clearances

- **CONFIDENTIAL** — Unauthorized disclosure could cause *damage* to national security. Granted via a Tier 3 investigation; least common at federal level.
- **SECRET** — Unauthorized disclosure could cause *serious damage* to national security. Granted via a Tier 3 (T3) investigation. The most common cleared role in industry.
- **TOP SECRET (TS)** — Unauthorized disclosure could cause *exceptionally grave damage* to national security. Granted via a Tier 5 (T5) investigation.

Layered Designations

- **SCI — Sensitive Compartmented Information** Not a separate clearance level. An access designation that sits on top of TS, controlling intelligence-sourced or methods-sensitive information. Same T5 investigation; additional adjudication and often a polygraph (CI Poly or Full-Scope/FSP) depending on the sponsoring agency.
- **SAP — Special Access Programs** Programs with controls beyond standard classification. Access is granted on a strict need-to-know basis after additional vetting and program briefings.
- **DOE Q & L Clearances** Department of Energy clearances for access to Restricted Data and other nuclear-related information. Q is roughly equivalent to TS; L is roughly equivalent to Secret.

02 • INVESTIGATION TIERS (LEGACY & CURRENT)

The federal government is currently transitioning from a 5-tier investigation framework (T1–T5) to a streamlined 3-tier model (Low / Moderate / High) under Trusted Workforce 2.0. Both models coexist today; legacy products are being phased out over the next several years.

Legacy 5-Tier Framework (Still in Use)

- **TIER 1 (T1)** Non-Sensitive, Low-Risk Public Trust positions — basic National Agency Checks and credit checks.
- **TIER 2 (T2)** Moderate-Risk Public Trust positions — employment, education, references, financial review.
- **TIER 3 (T3)** Non-Critical Sensitive — supports Confidential and Secret clearances. National Agency Checks, financial and criminal record review, employment verification.
- **TIER 4 (T4)** High-Risk Public Trust — full Background Investigation, similar in scope to clearance investigations but without the national-security focus.
- **TIER 5 (T5)** Critical and Special Sensitive — supports Top Secret, SCI, and SAP access. Formerly the SSBI (Single Scope Background Investigation). Includes detailed personal, professional, and financial review plus subject and reference interviews.

New 3-Tier Framework (Under TW 2.0)

- **LOW TIER** Consolidates legacy T1 and certain low-risk reviews. FY 2026 DCSA standard rate: roughly \$356.
- **MODERATE TIER** Consolidates T2 and T3. FY 2026 DCSA standard rate: roughly \$1,081.
- **HIGH TIER** Consolidates T4 and T5. FY 2026 DCSA standard rate: roughly \$6,155 (varies by product and add-ons).

Important: Investigation costs are paid by the sponsoring agency or employer through the DCSA Working Capital Fund. The applicant pays nothing — ever.

03 • THE CLEARANCE PROCESS TODAY

The clearance process has four phases under TW 2.0. The biggest change from the legacy model: once eligibility is granted, you stay enrolled in Continuous Vetting rather than waiting years for a periodic reinvestigation.

Phase 1 — Sponsorship

A clearance can only be initiated by a sponsoring federal agency or cleared employer with a contractual need. You cannot apply for a clearance on your own; there is no “self-sponsor” path. Loss of sponsorship without transfer to another sponsor will eventually result in clearance termination.

Phase 2 — Application (SF-86 → eApp → PVQ)

The Questionnaire for National Security Positions (SF-86) is the foundational application document, collecting personal history, employment, education, foreign contacts, finances, and criminal history. The SF-86 is now completed in eApp (the NBIS-based replacement for e-QIP). The new Personnel Vetting Questionnaire (PVQ) is rolling out by use case under NBIS and will eventually replace the SF-86.

Phase 3 — Background Investigation

DCSA (now responsible for roughly 95% of federal background investigations) conducts National Agency Checks, credit and criminal record reviews, employment and education verification, and — at the T5/High Tier — detailed personal and reference interviews. Interim eligibility can be granted on a limited record check while the full investigation proceeds.

Phase 4 — Adjudication

The adjudicating agency (the DoD Consolidated Adjudications Facility within DCSA for most DoD personnel, or agency-specific adjudicators for CIA, NSA, FBI, etc.) reviews investigation results against the 13 Adjudicative Guidelines: allegiance to the U.S., foreign influence, foreign preference, sexual behavior, personal conduct, financial considerations, alcohol consumption, drug involvement, psychological conditions, criminal conduct, handling of protected information, outside activities, and use of information technology. Adjudicators apply a “whole-person” analysis.

Phase 5 — Continuous Vetting (Ongoing)

Once granted, cleared individuals are enrolled in Continuous Vetting: automated, real-time checks against credit, criminal, court, and other public-record sources. CV alerts the security office to flagged events as they occur — not years later — enabling early intervention and reducing the need for traditional periodic reinvestigations.

04 • PUBLIC TRUST vs. NATIONAL SECURITY CLEARANCE

These are often confused but serve different purposes. A common myth: “Public Trust is a clearance.” It is not. Public Trust is a suitability designation, not a clearance to access classified information.

ASPECT	NATIONAL SECURITY CLEARANCE	PUBLIC TRUST
Purpose	Access classified national security information	Suitability for sensitive but unclassified roles
Levels	Confidential, Secret, Top Secret (+ SCI / SAP)	Low, Moderate, High Risk
Governing Body	DoD or sponsoring federal agency	Office of Personnel Management (OPM)
Investigation Focus	National security risk	Job suitability & trustworthiness
Citizenship	U.S. citizenship required	U.S. citizenship or permanent residency (often)
Portability	Reciprocal across most agencies (with verification)	Generally not portable; reassessed per agency

05 • MAINTAINING YOUR STANDING UNDER CONTINUOUS VETTING

Under TW 2.0, cleared personnel must self-report life events that could affect eligibility — they no longer wait for a five-year reinvestigation to surface them. Failure to self-report is itself a potential security concern.

What Continuous Vetting Monitors

- Credit data and major financial events (bankruptcies, judgments, significant delinquency)
- Criminal records and arrests at federal, state, and local levels
- Civil court records (lawsuits, certain judgments)
- Public-record terrorism, foreign influence, and counterintelligence indicators
- Eligibility status across agencies (via DISS / NBIS data sharing)

Reportable Events (SEAD 3)

Security Executive Agent Directive 3 establishes self-reporting requirements. Common reportable events include: foreign travel, foreign contacts, marriage or cohabitation, financial issues, arrests or detentions, drug or alcohol issues, mental health hospitalization, media contact about classified work, attempts at elicitation, and changes in citizenship status.

Common Reasons for Denial or Revocation

- **Financial considerations** — unresolved debts, bankruptcies, gambling, unexplained affluence.
- **Foreign influence or preference** — close ties to foreign nationals or governments, dual citizenship issues.
- **Personal conduct** — dishonesty during the process, falsified documents, omissions on the SF-86.
- **Criminal conduct** — recent arrests, patterns of poor judgment, undisclosed offenses.
- **Drug involvement** — illegal use, including marijuana under federal law regardless of state legality.
- **Mishandling of protected information** — spillage, improper storage, unauthorized disclosure.

06 • KEY SYSTEMS & AGENCIES

- **DCSA — Defense Counterintelligence and Security Agency** Conducts roughly 95% of federal background investigations; oversees industrial security under NISPOM and the DoD CAF.
- **DoD CAF — Consolidated Adjudications Facility** Now an organization within DCSA. Reviews investigations and makes eligibility determinations for DoD personnel and contractors.
- **DISS — Defense Information System for Security** Current DoD enterprise system for managing clearance eligibility, visit requests, and access. Being phased out in favor of NBIS.
- **NBIS — National Background Investigation Services** The end-to-end replacement system: application (eApp/PVQ), investigation, adjudication, and continuous vetting in one platform. Full deployment projected by FY2028.
- **Scattered Castles** The Intelligence Community's clearance verification system, separate from DISS/NBIS. Used by CIA, NSA, FBI, NSA, DIA, and others.

07 • RECIPROCITY & PORTABILITY

Federal policy generally supports clearance reciprocity — your eligibility transfers across most agencies. In practice, the new sponsoring agency may still require verification, additional checks, or agency-specific access conditions (most commonly, polygraphs for IC roles or additional briefings for SAP access).

- National Security Clearances: typically reciprocal between federal agencies, with verification lag.
- SCI and SAP access: often re-adjudicated or require additional polygraphs (CI Poly, FSP) per agency-specific guidelines.
- Public Trust: generally not portable — each agency reassesses suitability independently.
- Break in service > 24 months: typically requires a new SF-86/PVQ and may require a new investigation.

ABOUT THIS GUIDE

Informational baseline only. Federal policy continues to evolve under Trusted Workforce 2.0 — verify current requirements with your FSO or sponsoring agency.

Sources: DCSA, ODNI, OPM, TW 2.0 reports.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

DoD CYBER WORKFORCE

DCWF, DoDM 8140.03, and Your Certification Path

UPDATED MAY 2026 • VERSION 2.0

DoD cyber workforce policy has fundamentally changed. The old **DoD 8570.01-M** framework with its IAT / IAM Level I, II, and III categories was officially cancelled on February 15, 2023. The successor — **DoD Manual 8140.03** — replaces broad certification "levels" with a role-based qualification model under the DoD Cyber Workforce Framework (DCWF).

WHAT CHANGED

- **DoD 8570.01-M Cancelled** Officially superseded by DoDM 8140.03 on February 15, 2023. The IAT and IAM Level I, II, and III categorization is no longer the operative framework.
- **Role-Based, Not Level-Based** Qualifications now map to specific DCWF work roles (70+ total across 7 workforce elements), each with Basic, Intermediate, or Advanced proficiency requirements.
- **Your Certifications Still Count** Security+, CISSP, CySA+, CEH, GIAC, and CompTIA credentials remain valid — but how they qualify you is now determined by the DCWF work role you're filling, not a generic "Level II" label.
- **Compliance Deadlines Are Live** Cybersecurity element foundational qualifications were due February 15, 2025. IT, Cyber Effects, Intelligence (Cyber), and Cyber Enablers are due February 15, 2026. Cybersecurity resident qualifications follow February 15, 2027.

CONTENTS

01	The Shift from 8570 to 8140	Page 2
02	The DCWF Framework — Elements, Roles, Proficiency	Page 2
03	Qualification Pathways — Foundational vs. Resident	Page 3
04	Certifications That Still Drive Cleared Cyber Hiring	Page 3
05	Beginner's Roadmap into Cleared Cyber / IT	Page 4
06	Implementation Timeline & What It Means For You	Page 4

01 • THE SHIFT FROM 8570 TO 8140

For nearly two decades, DoD 8570.01-M defined cyber workforce qualifications through a simple grid: two categories (IAT for technical roles, IAM for management) and three levels each (I, II, III). A handful of commercial certifications mapped to each cell. It was straightforward — and increasingly outdated.

Why 8570 Was Retired

- Cyber roles grew far faster and more specialized than the IAT/IAM grid could capture (cloud, DevSecOps, threat hunting, AI/ML security, OT/ICS security).
- The framework rewarded credential collection over demonstrated capability — the certification didn't necessarily match what the person actually did on the job.
- It excluded large parts of the broader cyber workforce: cyber intelligence analysts, software developers building secure code, data scientists supporting cyber missions, program managers running cyber acquisitions.
- DoD needed a framework that could absorb new specialties as they emerged, instead of waiting for the next manual revision.

What DoDM 8140.03 Does Differently

- **Defines role-specific KSATs.** Each work role has documented Knowledge, Skills, Abilities, and Tasks (KSATs) describing what the person actually does.
- **Anchors to capability, not credentials.** Qualifications can be met through education, training, commercial certification, on-the-job experience, or military training — whichever pathway demonstrates the required KSATs.
- **Expands the scope.** Covers seven workforce elements, not just IT and IA. Includes cyber effects, intelligence, software engineering, data/AI, and enablers.
- **Builds in agility.** New work roles can be added to the DCWF as the threat and mission landscape evolves — without a full directive rewrite.

02 • THE DCWF FRAMEWORK

The DoD Cyber Workforce Framework (DCWF) is the standardized lexicon DoD uses to identify, track, and qualify every cyber-coded position across military, civilian, and contractor populations. Three concepts to know: workforce elements, work roles, and proficiency levels.

Seven Workforce Elements

- **Information Technology (IT)** System administration, network operations, infrastructure, enterprise IT.
- **Cybersecurity (CS)** Defensive operations, vulnerability management, incident response, security engineering, governance.
- **Cyber Effects (CE)** Offensive operations, cyber operations planning, cyberspace operations.
- **Intelligence (Cyberspace)** All-source cyber intelligence analysis, target development, exploitation analysis.
- **Data / Artificial Intelligence (Data/AI)** Data science, machine learning, AI engineering in cyber and mission contexts.
- **Software Engineering (SE)** Secure software design, development, testing, and DevSecOps in DoD environments.
- **Cyber Enablers** Acquisition, program management, training, legal, policy, and other roles supporting the cyber mission.

Work Roles & Proficiency

Across those seven elements, the DCWF currently defines roughly 70+ work roles. Each role lists its required KSATs at three proficiency levels:

- **BASIC** Entry-level competence. Performs work under supervision; foundational understanding of role-specific tasks.
- **INTERMEDIATE** Independent practitioner. Executes role responsibilities with minimal oversight; mentors junior team members.
- **ADVANCED** Senior expert. Leads complex initiatives, drives strategy for the work role, and develops the next generation of practitioners.

03 • QUALIFICATION PATHWAYS — FOUNDATIONAL vs. RESIDENT

DoDM 8140.03 separates qualifications into two complementary categories. Foundational qualifications establish your baseline capability to enter the role. Resident qualifications validate that you can demonstrate the role's KSATs in the actual job environment.

Foundational Qualifications

These prove you have the underlying knowledge and skills before stepping into the role. Acceptable options can include any of the following, as listed in the DoD 8140 Qualification Matrix at [cyber.mil](#):

- Approved commercial certifications (Security+, CISSP, CySA+, GIAC certs, vendor credentials, etc.)
- DoD-owned training courses (FedVTE, service-specific cyber schools, DCITA courses)
- Formal education (degrees from CAE-CD/CO/R designated institutions, NSA-sponsored programs)
- Military training and occupational specialty experience
- Demonstrated equivalent experience under documented review

Resident Qualifications

Foundational status gets you in the door; resident status confirms you can do the job once you're there. Resident qualifications are demonstrated on-the-job: completed training in the actual role, supervisor sign-off on KSAT execution, and continued professional development. Deadlines for resident qualifications follow foundational deadlines by approximately two years for each workforce element.

Source of Truth: The authoritative DoD 8140 Qualification Matrix lives at [cyber.mil](#). Components and contracts can impose stricter standards — always verify your specific role requirements with your hiring authority or FSO.

04 • CERTIFICATIONS THAT STILL DRIVE CLEARED CYBER HIRING

The certifications listed below remain widely accepted under DoDM 8140.03 — but they now qualify holders for specific DCWF work roles rather than generic IAM/IAT levels. The table below maps high-value certifications to the workforce elements where they carry the most weight.

WORKFORCE ELEMENT	HIGH-VALUE CERTIFICATIONS
Information Technology (IT)	CompTIA A+, Network+, Linux+ • Cisco CCNA / CCNP • Red Hat RHCSA • Microsoft Azure / AWS / GCP foundational certs
Cybersecurity (CS)	CompTIA Security+, CySA+, PenTest+, SecurityX (formerly CASP+) • ISC2 CISSP, SSCP, CCSP • ISACA CISM, CISA • GIAC GSEC, GCIH, GCIA, GCED • EC-Council CEH
Cyber Effects (CE)	OSCP, OSCE, OSEP • GIAC GPEN, GXPN, GREM • CEH Master / CPENT • CISSP (for leadership-track effects roles)
Intelligence (Cyberspace)	GIAC GCTI, GCFA, GREM, GNFA • CISSP • IC-specific training (per agency)
Data / AI	CompTIA Data+, DataX • AWS / Azure / Google ML & Data Engineering certs • Cloudera, Databricks credentials • Vendor-neutral AI/ML certifications (emerging)
Software Engineering (SE)	ISC2 CSSLP • GIAC GWEB, GSSP • AWS / Azure DevOps Engineer • Kubernetes (CKA / CKAD / CKS) • Scaled Agile (SAFe), CSM
Cyber Enablers	PMP, CAPM • ITIL 4 • ISACA CGEIT, CRISC • FAC-COR, DAWIA credentials • CMMC AB credentials (CCP, CCA)

05 • BEGINNER'S ROADMAP INTO CLEARED CYBER / IT

If you're entering the cleared cyber or IT workforce from scratch — transitioning out of the military, finishing school, or pivoting from a non-technical field — here's a no-nonsense progression that aligns with how the DoD 8140 framework actually hires.

Step 1 • Lay the Groundwork

- **CompTIA A+** Hardware, software, basic troubleshooting. The foundational IT credential.
- **CompTIA Network+** Networking fundamentals — essential for nearly any DoD cyber or IT role.
- **CompTIA Security+** The most widely required entry-level cyber credential for cleared work; maps to many DCWF Basic-level cybersecurity roles.

Step 2 • Pick a DCWF Work Role

Browse the DCWF work role catalog at cyber.mil. Pick one or two roles that match what you actually want to do day-to-day. Common starter roles: Systems Administration (IT), Network Operations (IT), Cyber Defense Analyst (CS), Vulnerability Assessment & Management (CS), All-Source Analyst (Intelligence).

Step 3 • Land an Entry-Level Cleared Role

- Help Desk / IT Support — ideal for clearance sponsorship while you build experience
- Junior Systems Administrator or Network Operations roles
- SOC Tier 1 / Cyber Defense Analyst — widely available, strong career progression
- DoD SkillBridge internships (last 180 days of military service — high-leverage path)

Step 4 • Stack Credentials and Experience

- CySA+ or GSEC for analyst-track progression
- PenTest+ or GPEN for offensive-track progression
- CISSP once you have 5+ years across two or more security domains (the single most impactful cert in cleared cyber)
- Cloud certifications (AWS / Azure) — increasingly required as DoD migrates to cloud

06 • IMPLEMENTATION TIMELINE & WHAT IT MEANS FOR YOU

DoDM 8140.03 sets phased compliance deadlines by workforce element. If you're currently in a coded DoD cyber role — or applying for one — these dates matter.

- **February 15, 2025 (Past)** Foundational qualifications deadline for the Cybersecurity workforce element.
- **February 15, 2026** Foundational qualifications deadline for IT, Cyber Effects, Intelligence (Cyber), and Cyber Enablers elements.
- **February 15, 2027** Resident qualifications deadline for the Cybersecurity workforce element.
- **Following years** Resident qualification deadlines for the remaining elements; Data/AI and Software Engineering elements continue rolling implementation.

*If your role is coded under the DCWF and you're not yet qualified, your component is required to bring you into compliance — typically through training, certification, or documented experience review. **Your IAM, ISSM, or FSO is the right starting point.***

ABOUT THIS GUIDE

Informational baseline only. The DoD 8140 Qualification Matrix at cyber.mil is the authoritative source — verify role-specific requirements with your IAM, ISSM, or FSO.

Sources: DoD CIO, cyber.mil, DoDM 8140.03.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

GOVCON FOUNDATIONS

Your Starter Guide to Government Contracting

UPDATED MAY 2026 • VERSION 2.0

Government contracting (GovCon) has its own vocabulary, its own rhythm, and its own rules. **This guide is a plain-English baseline** covering how the industry actually works, what contract types look like in practice, the realities of job stability on a contract, and how to break in even if you don't have direct experience or a clearance yet.

WHAT YOU'LL FIND IN THIS GUIDE

- **How GovCon Actually Works** The terms, the players, and the contract structures that shape every cleared role in the industry.
- **Job Stability Realities** The myths, the truths, and what happens when contracts recompetes or change hands.
- **Breaking In Without Experience** How to position yourself, what entry points exist, and how clearance sponsorship actually works.
- **Smart Questions Before You Sign** The recruiter questions that protect you from surprises after you've accepted.

CONTENTS

01	How GovCon Actually Works — Key Terms	Page 2
02	The Contract Lifecycle — Award to Re compete	Page 2
03	Job Stability Realities (Myths vs. Truths)	Page 3
04	Breaking In Without Experience	Page 3
05	Entry Points & Clearance Sponsorship	Page 4
06	Smart Questions to Ask Before You Sign	Page 4

01 • HOW GOVCON ACTUALLY WORKS

Government contracting is the system by which federal agencies buy services and products from private companies. Two layers of companies usually do the work: the prime contractor (who holds the contract directly with the government) and one or more subcontractors (who support the prime). Understanding this structure — and the vocabulary around it — is essential to navigating any cleared role.

Key Terms You'll Hear Constantly

- **GOVCON** Government Contracting. The broad industry where private companies deliver services or products to federal agencies under contract.
- **PRIME CONTRACTOR** The company holding the main contract with the government. Examples: Leidos, Booz Allen Hamilton, CACI, ManTech, SAIC, Lockheed Martin, Northrop Grumman.
- **SUBCONTRACTOR (SUB)** A company that supports the prime by filling specific roles or delivering specific work. Subs are chosen by the prime based on capabilities, set-aside status, or past relationships.
- **CUSTOMER / CLIENT** The government agency that owns and oversees the contract — e.g., DoD, NSA, NGA, DIA, CIA, DHS, NIH.
- **IDIQ** Indefinite Delivery / Indefinite Quantity. A flexible contract structure where the government commits to a ceiling value but issues specific work over time as needs change.
- **TASK ORDER (TO)** A specific assignment issued under an IDIQ contract — the actual scope of work, timeline, and budget for a discrete project.
- **OPTION YEAR (OY)** An additional year the government can extend a contract beyond its base period. Most contracts have a base year plus 3–4 option years.
- **GWAC** Government-Wide Acquisition Contract. Multi-agency IDIQ vehicles like OASIS+, GSA Alliant 3, NASA SEWP VI, and others, used by federal agencies to buy services efficiently.
- **DISS** Defense Information System for Security — the DoD system that tracks clearance eligibility and access. Being phased out in favor of NBIS (National Background Investigation Services).

02 • THE CONTRACT LIFECYCLE

Most cleared roles tie directly to a specific contract — your job exists because the work exists on the contract. Understanding where a contract sits in its lifecycle tells you a lot about role stability and growth potential.

The Three Phases

- **AWARD** After a competitive bid, a contract is awarded to one or more contractors. When a company wins, hiring typically accelerates rapidly to staff the contract before performance begins.
- **PERFORMANCE** The base year and any option years where the contractor delivers against the contract scope. This is where most cleared work happens — typically 3 to 5 years total.
- **RENEWAL or RECOMPETE** Toward the end of the contract, the agency decides whether to extend (option year) or recompete (open bidding for a new contract). If a different contractor wins the recompete, they typically absorb most existing cleared staff — the work needs the people who already do it.

03 • JOB STABILITY REALITIES

GovCon careers look different from private-sector ones — in ways that often turn out to be more stable, not less. The same five or ten years of work might involve two or three different employers on the same physical seat at the same customer site. Here are the most common misconceptions, with the actual reality.

MYTH *Contracts can end at any time, leaving you stranded.*

REALITY Federal contracts have defined terms (base year plus option years) and aren't typically cut short without cause. Contractors actively work to deliver well so option years are exercised and recompetes are won.

MYTH *If the contract changes hands, you lose your job.*

REALITY Most cleared staff are retained by the incoming contractor when contracts change hands — your clearance, customer relationships, and institutional knowledge are too valuable to lose. You may change badges; the work usually stays.

MYTH *Government shutdowns automatically furlough contractors.*

REALITY Funded contracts continue during shutdowns. Many cleared roles — especially in defense and intelligence — are funded through multi-year appropriations and continue largely unaffected.

MYTH *Subcontractors are less stable than primes.*

REALITY Subs are often more stable in the day-to-day. They're hired for specific Task Orders and tend to keep those positions through the life of the TO. Primes can shift personnel around more aggressively.

What Actually Drives GovCon Stability

- Your clearance — active, current, and aligned to the customer's needs.
- Your role on the contract — mission-critical positions are recompile-safe.
- Your customer relationship — government program managers vote with their voice when contracts recompile.
- The agency's mission posture — IC, DoD, and cybersecurity-coded work is on a long-term growth trajectory.

04 • BREAKING IN WITHOUT EXPERIENCE

If you're new to GovCon — no clearance, no defense background, no contract experience — it can feel like a closed system. It's not. It's a system with specific entry points that reward persistence and the right positioning.

Step 1 • Speak the Language

Recruiters and hiring managers are scanning for industry vocabulary. Reframe your existing experience using GovCon terms: “program support,” “compliance documentation,” “contract deliverables,” “stakeholder coordination,” “technical writing for federal customers.” The work you've done probably maps; the language just needs to align.

Step 2 • Identify Transferable Skills

- Project management, scheduling, deliverables tracking
- Administrative skills, document management, compliance records
- Technical aptitude (IT support, networking, software, data)
- Military service, federal civilian experience, public-sector roles — directly transferable

Step 3 • Earn a Foundational Certification

- CompTIA Security+ — the single most useful cert for breaking into cleared IT/cyber
- PMP or CAPM — strong signal for program coordination and management-track roles
- ITIL Foundation — useful for IT service management roles
- Industry-specific (acquisition, compliance, cyber) certifications relevant to your target work

05 • ENTRY POINTS & CLEARANCE SPONSORSHIP

Not every cleared role requires you to walk in already cleared. Some categories of work are entry-level by design, and some companies are actively in the business of investing in talent and sponsoring clearances. Knowing where to aim makes the difference.

Best Entry-Level Roles

- **Help Desk / IT Support** Often does not require clearance to start; ideal for clearance sponsorship after 6–12 months of solid performance.
- **Administrative Assistant / Program Coordinator** Support contract teams with scheduling, documentation, deliverables tracking. Strong gateway role.
- **Junior Data / Financial / Operations Analyst** Analyst-track positions on large contracts. Companies often invest in clearance after onboarding.
- **SOC Tier 1 / Cyber Defense Analyst** Entry into cleared cyber work; often requires Security+ and a willingness to start at night-shift or rotating schedule.
- **Military to Federal Transition Programs** DoD SkillBridge, Hiring Our Heroes Corporate Fellowship, MSSA, FourBlock — high-leverage paths for transitioning service members.

How Clearance Sponsorship Actually Works

Companies are reluctant to sponsor clearances cold — it's expensive and uncertain. The realistic path: take a role that doesn't require a clearance, perform exceptionally for 6–18 months, and then request to be sponsored for work that does. Clearance sponsorship is a reward for proven employees, not an entry-level perk.

06 • SMART QUESTIONS TO ASK BEFORE YOU SIGN

The single biggest source of GovCon regret is accepting a role without understanding the structure underneath it. These are the questions a confident candidate asks — not pushy, just informed.

About the Role & Contract

- Is the company a prime or a sub on this contract?
- What contract is this role tied to, and what option year is it in?
- Who is the customer agency, and which program office?
- What's the work location? Onsite / hybrid / remote, and are there travel or deployment expectations?

About Compensation & Schedule

- Is the position exempt or non-exempt? Salaried or hourly?
- What's the work schedule — standard 80-hour biweekly, 84-hour shift, or rotating?
- Are there shift differentials for nights, weekends, or holidays?
- What's the full compensation picture — base, bonuses, relocation, retirement match, PTO?

About Clearance & Commitment

- How is the clearance process handled, and does the company sponsor upgrades?
- Is there a non-compete clause tied to this contract or program?
- How long has the company held this contract, and when does the next recompetes happen?

ABOUT THIS GUIDE

Informational baseline only. Specific terms, vehicles, and clearance requirements vary by contract and customer — always verify with your recruiter or hiring company.

Related guides: Security Clearances, DoD Cyber Workforce, Career Toolkit.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

COMPENSATION PLAYBOOK

Understanding Pay, Schedules, and Negotiation in GovCon

UPDATED MAY 2026 • VERSION 2.0

Cleared compensation has its own logic — hourly roles marketed as salary, 84-hour biweekly schedules, shift differentials that stack, and a clearance premium that meaningfully outpaces non-cleared base pay. This guide is your baseline: how pay structures work, what current cleared salaries look like in 2026, and how to negotiate effectively without burning bridges in a small, connected industry.

2026 CLEARED COMPENSATION AT A GLANCE

- All-Time High Average: \$126,125 (2026 ClearanceJobs Security Clearance Compensation Report) — nearly 6% YoY growth. 70% of cleared professionals received salary increases in 2025; 12% received raises of more than 10%.
- By Clearance Level: DoD Top Secret averages \$126,839 · TS/SCI averages \$139,261 · Full-Scope Polygraph carries a further premium.
- Market Context: Compensation rose despite return-to-office mandates, agency restructuring, and federal workforce uncertainty — a clear signal that demand for cleared talent remains strong.
- The Takeaway: Your clearance remains one of the most valuable credentials in today's labor market — and the data backs negotiating accordingly

CONTENTS

01	Pay Structures — Exempt, Non-Exempt, and the "Salary" Trap	Page 2
02	Schedules — 80, 84, Panama, and Rotating Shifts	Page 2
03	Shift Differentials & Premium Pay	Page 3
04	Knowing Your Market Value	Page 3
05	The Negotiation Playbook — Before, During, After	Page 4
06	The Contract-Hopping Trap (Don't Burn Bridges)	Page 4

01 • PAY STRUCTURES — EXEMPT, NON-EXEMPT, AND THE "SALARY" TRAP

The most common pay-structure surprise in GovCon: roles marketed as "salary" that are actually salary non-exempt — you're paid hourly for every hour worked, but without overtime premium. Understanding the structure of your role is the foundation of compensation literacy.

Salary Exempt

A fixed annual salary paid regardless of hours worked. Most professional and management positions. No overtime pay even when you work more than 40 hours. Your salary is the salary.

Salary Non-Exempt

An hourly rate marketed and structured like a salaried role — you're paid for every hour worked, but there's typically no time-and-a-half overtime premium for hours beyond 40. Common on shift-based contracts. Pay can vary biweekly based on actual hours.

Hourly / W-2 Contractor

Straight hourly compensation, often with full benefits. Overtime rules depend on exempt status and contract terms.

1099 / Independent Contractor

Self-employed contractor structure. Higher hourly rate to account for self-paid taxes, benefits, and overhead. Common in specialized cleared consulting; less common in line cleared roles.

CONUS vs. OCONUS

- **CONUS (Continental U.S.)** Standard domestic rates aligned with cost of living and government labor standards. The baseline.
- **OCONUS (Outside Continental U.S.)** Higher hourly rates typically reflect overseas allowances, hazard pay in high-risk zones, hardship differentials, and tax advantages (Foreign Earned Income Exclusion may apply).

02 • SCHEDULES — 80, 84, PANAMA, AND ROTATING SHIFTS

Cleared work frequently runs on schedules other than standard 40-hour weeks. Mission coverage doesn't stop for weekends. Understanding the schedule before you accept is essential — it directly affects your biweekly pay.

Standard 80-Hour Biweekly

Traditional Monday–Friday, 40 hours per week, 80 hours per pay period. Most analyst, engineering, and management roles.

84-Hour Biweekly

Common on shift-based mission roles requiring continuous coverage. You work 84 hours over two weeks instead of 80 — paid at your hourly rate for all 84 hours.

Panama Schedule (2-2-3)

2 days on, 2 days off, 3 days on — totaling 84 hours over two weeks. Used for 24/7 mission coverage. Example: at \$50/hour, biweekly pay is $\$50 \times 84 = \$4,200$.

12-Hour Rotating

Twelve-hour shifts in rotation (often 4 days on / 4 days off). Two weeks adds up to roughly 84 hours. Common in SOC's, OPS centers, and mission watch floors.

24/7 Coverage

Continuous coverage with rotating morning, swing, and night shifts. Usually 84-hour biweekly cycles. Shift differentials almost always apply.

03 • SHIFT DIFFERENTIALS & PREMIUM PAY

Many contracts add premium pay on top of base hourly rate for shifts worked at non-standard times. These differentials are negotiable on some contracts and fixed on others — always ask before you accept.

Common Differentials

- **Night Shift Differential** Typically 5–10% above base for evening or overnight shifts. Example: \$50 base + 10% = \$55/hour at night.
- **Weekend Pay** Saturday and Sunday premium, often \$2–\$5/hour or a fixed percentage. Example: \$50 base + \$3 weekend = \$53/hour.
- **Holiday Pay** Federal holidays worked typically pay 15–20% above base. Example: \$50 base + \$10 holiday = \$60/hour.
- **Hazardous Duty / Combat Zone** OCONUS in designated combat zones can carry significant additional pay, plus potential tax exclusions on portions of income.

Stacking Differentials

Differentials usually stack. A Sunday-night holiday shift in a 24/7 mission environment can combine night + weekend + holiday for a sizeable hourly multiplier. Example: \$50 base + \$5 night + \$10 holiday = \$65/hour on a holiday night.

Contract Margins Affect Your Pay Ceiling

The contract type drives how much room there is for negotiation. Generally:

- **Cost-Plus Contracts (typical margins 8–15%)** Government reimburses costs plus a set fee. Tighter pay ceilings.
- **Fixed-Price Contracts (typical margins 15–25%)** Contractor takes cost-overflow risk; more negotiation flexibility.
- **Labor-Intensive Subcontracts (typical margins 20–30%)** Cleared cyber, AI, and specialized technical fields. Highest negotiation room.

04 • KNOWING YOUR MARKET VALUE

Negotiation without data is just hope. Before any compensation conversation, gather objective evidence of what your specific combination of clearance, certifications, and experience commands in the current market.

Data Sources Worth Using

- **ClearanceJobs Salary Calculator** Tailored salary trends by role, location, clearance level, and polygraph. Most useful single tool for cleared compensation benchmarking.
- **2026 Security Clearance Compensation Report** ClearanceJobs' annual industry-wide survey — breakdowns by state, occupation, clearance level, education.
- **Government Contractors Compensation Survey** Detailed data for 700+ specific roles across GovCon companies.
- **Listed Salary Ranges** Salary transparency laws now cover 50%+ of U.S. workers — most job postings include ranges. Compare across similar listings for triangulation.
- **Peer Conversations** Recruiters, mentors, and peers with similar profiles. Often the most accurate signal for what real offers look like.

05 • THE NEGOTIATION PLAYBOOK

Effective negotiation is preparation, communication, and follow-through. The goal isn't to extract every last dollar; it's to land on an offer that reflects your actual value and that you can commit to without resentment six months in.

Before the Negotiation

- **Know your floor and your target.** Floor = lowest you'll genuinely accept. Target = realistic market-aligned ask. Use the data sources above to ground both numbers.
- **Map the total compensation, not just base.** Health insurance, retirement match, PTO, bonus structure, relocation, training budget, clearance upgrade investment — all of it matters.
- **Understand the contract context.** Cost-plus contracts have tighter ceilings than fixed-price ones. The labor category your role maps to has a documented rate range.

During the Negotiation

- **Lead with enthusiasm, follow with data.** "I'm excited about this role and the team. Based on [data source], roles with my clearance and certification profile in this market typically range from X to Y — can we discuss?"
- **Anchor on the total, not the base alone.** If base is fixed by the labor category, negotiate signing bonus, relocation, PTO, certification reimbursement, or accelerated review.
- **Be honest about competing offers.** If you have one, say so professionally. If you don't, don't invent one — the cleared community is small.

After the Negotiation

- **Get it in writing.** Every term — base, bonus, PTO, sign-on, relocation, start date. If it's not in the offer letter, it doesn't count.
- **Read the fine print.** Non-compete clauses, clearance hold provisions, repayment clauses on sign-on bonuses, and contract-portability language.
- **Send a written acceptance.** Brief, professional, restates the key terms. Closes the loop and demonstrates you take the commitment seriously.

06 • THE CONTRACT-HOPPING TRAP

The GovCon community is small and tightly connected. Program managers, recruiters, and security officers talk — across companies, across contracts, across years. Actions that look like short-term wins can cost you long-term.

CAUTIONARY EXAMPLE *Dual Submission on the Same Contract*

You accept a Conditional Offer Letter with Company A; they submit your profile to the customer for a high-profile contract. A week later, Company B offers you the same contract at a slightly higher rate — you accept and they submit you too.

Result: The customer sees dual submissions, removes you from consideration entirely, and both companies are informed. The program manager remembers. Within weeks, the broader cleared community knows. Future opportunities on related programs quietly disappear.

The Bottom Line

- Shop around before you commit — that's smart, not shady.
- Once you accept a Conditional Offer Letter (COL), don't shop the same contract with another company.
- If you change your mind after signing, notify the employer professionally and immediately — don't ghost.
- Honor the commitments you make; reputation compounds across decades in GovCon.

ABOUT THIS GUIDE

Informational baseline only. Compensation figures based on 2026 ClearanceJobs data; specific offers vary by contract, customer, location, and individual qualifications. **Sources:** ClearanceJobs 2026 Comp Report, BLS, Deltek Clarity Study.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

THE CAREER TOOLKIT

Resumes, Recruiters, and the Cleared Job Search

UPDATED MAY 2026 • VERSION 2.0

Two things move the needle most in a cleared job search: **a resume that earns the second look** and **a recruiter relationship that actually advocates for you**. This guide is a baseline for both: how to write resumes that get past ATS screens and onto desks, and how to work with recruiters strategically while spotting the red flags.

CORE PRINCIPLES

- **Lead with your clearance.** In cleared work, your clearance is the headline. Put it next to your name, not buried at the bottom.
- **Quantify everything.** "Reduced incident response time by 40%" beats "Effectively managed incidents" every single time.
- **Treat recruiters as partners, not gatekeepers.** Good recruiters open doors you can't see; bad ones waste your time and protect their commission. Know the difference.
- **Never share your SSN or banking info early.** Legitimate recruiters don't need it before a formal offer and onboarding. Treat any early request as a red flag until proven otherwise.

CONTENTS

01	Resume Fundamentals — Contact, Format, Structure	Page 2
02	Content That Converts — Summary & Bullet Formula	Page 2
03	Certifications, Skills & Tailoring for the Role	Page 3
04	Working With Recruiters — Types & How They Help	Page 3
05	Recruiter Red Flags — What to Watch For	Page 4
06	The Tier One 10 — Non-Negotiable Resume Rules	Page 4

01 • RESUME FUNDAMENTALS

Cleared hiring managers and recruiters scan, they don't read. Your resume has roughly 6–10 seconds to communicate who you are, what clearance you hold, and why you fit. Everything below serves that goal.

Contact Block — What Belongs

- **Name** Bold and prominent. Follow immediately with your clearance level if applicable: **Jane Doe | TS/SCI w/ FSP**
- **Location** City and state only (e.g., Washington, D.C.). Full street address is unnecessary and a privacy risk.
- **Phone** Mobile only. One number.
- **Professional email** firstname.lastname@gmail.com or similar. Skip the high school AOL handle.
- **LinkedIn (optional)** Only if it's current and matches your resume. Inconsistencies are a red flag for recruiters.

Contact Block — What Does NOT Belong

- Date of birth, SSN, full street address — privacy risks, never required.
- Photographs — standard in some countries, problematic in U.S. federal hiring.
- Hobbies, marital status, "References available upon request" — outdated filler.

Format Rules

- Professional fonts only: Calibri, Arial, Times New Roman, Helvetica. 10–12 pt body, larger headers.
- Present tense for your current role; past tense for everything else.
- Bullets over paragraphs. Recruiters don't read essays.
- Save and submit as PDF unless explicitly told otherwise. PDF preserves formatting across systems.
- Two pages is the new standard for mid-career and above; one page only for very early career or specific executive summaries.

02 • CONTENT THAT CONVERTS

The Summary Section

No need to label it "Professional Summary" — just dive in. Two to five tight sentences that capture your clearance, years of experience, technical depth, and the kind of value you deliver. Avoid generic adjectives ("results-driven," "dynamic," "motivated"); they signal nothing and waste prime real estate.

Example:

IT professional with 8+ years designing and managing secure enterprise networks. Expertise optimizing infrastructure for 99.9% uptime, implementing cloud architectures, and delivering scalable solutions. Active TS/SCI w/ FSP. Strong track record of driving efficiency in mission-critical environments.

The Bullet Point Formula

Strong resume bullets follow a simple structure: Action Verb + Task or Responsibility + Measurable Impact. Drop the fluff.

Weak: Effectively communicated with team members to achieve goals.

Strong: Led a cross-functional team of 10 to deliver a \$1.2M cloud migration two weeks ahead of schedule, reducing infrastructure costs 18%.

03 • CERTIFICATIONS, SKILLS & TAILORING

Where to List Certifications

For IT, cyber, and technical cleared roles, list your certifications immediately under the summary — not at the bottom. Hiring managers and ATS screens both prioritize them. For non-technical cleared roles (program management, analysis, operations), certifications belong near the bottom with education.

Group, Don't Dump

Don't list 40 certifications in a single paragraph. Group them logically and use " | " separators to save space:

- **Cybersecurity:** CISSP | CISM | CompTIA Security+ | GIAC GCIH
- **Cloud:** AWS Solutions Architect | Azure Solutions Architect Expert | Google Cloud Professional
- **Networking:** CCNA | CCNP | CompTIA Network+

Tailor for Every Application

- Mirror the job description's language — if the posting says "vulnerability management," don't write "vuln scanning."
- Move the most relevant experience and skills to the top of each section.
- Match keywords for ATS pass-through, but write authentically. Keyword stuffing fails human reviewers and modern ATS alike.
- If using AI tools (ChatGPT, Claude, etc.) to draft or refine, proofread carefully — generic AI phrasing is increasingly easy to spot and signals lack of effort.

Career Gaps — Be Brief, Be Honest

Don't hide gaps. A one-line acknowledgment is enough: "2023–2024: Career break for caregiving responsibilities." Recruiters appreciate honesty far more than creative rephrasing or unexplained jumps.

04 • WORKING WITH RECRUITERS

Recruiters fall into several categories — each operates differently, and understanding the differences helps you set expectations and engage productively.

Recruiter Types

- **Internal (Corporate) Recruiters** Work directly for the hiring company. Deep insight into culture and process; focused on filling that company's roles only.
- **External / Agency Recruiters** Represent multiple clients. Broader market view; sometimes more transactional.
- **Third-Party / Contingency Recruiters** Paid by the employer only when a placement happens. Often have direct hiring-manager access and can bypass the ATS entirely.
- **Retained Recruiters / Headhunters** Exclusively engaged for senior or hard-to-fill roles. Work on retainer; deeper engagement per candidate.
- **RPO (Recruitment Process Outsourcing)** A vendor running the employer's entire recruitment function. Long-term, brand-aligned engagement.

What Good Recruiters Do For You

- Provide resume feedback aligned to the specific role and company.
- Prep you for interviews with insight on the hiring manager, team, and culture.
- Advocate during compensation negotiation, leveraging market data.
- Bypass the ATS — your resume lands on a decision-maker's desk.
- Surface roles that never get posted publicly.

05 • RECRUITER RED FLAGS

The cleared community is small and reputable recruiters are easy to verify. Spotting a bad actor early saves you weeks of wasted time — and protects your personal data from being misused.

Walk Away If You See These

- **Requests for personal information too soon.** SSN, banking info, copy of your ID, full address — never share these before a formal offer and verified onboarding process.
- **Pressure to sign a Right-to-Represent (R2R) without details.** R2Rs grant exclusive submission rights for a specific role. Legitimate ones list the company, position, and scope. Vague or pressure-driven R2Rs are a hard pass.
- **Refusal to disclose the hiring company or contract details.** Some discretion is normal early in the process; complete refusal to name the customer or company even after initial conversations is a red flag.
- **Suspicious contact details.** Generic email domains, foreign phone numbers, no verifiable LinkedIn presence, no visible company website. Verify before engaging.
- **Unrealistic offers.** If the salary is dramatically above market for the clearance and skillset, dig in. "Too good to be true" is usually exactly that in cleared work.
- **Charging the candidate a fee.** Recruiters are paid by employers, not candidates. The only legitimate exception is rare executive headhunting at the senior C-suite level.

06 • THE TIER ONE 10 — NON-NEGOTIABLE RESUME RULES

Twenty-seven rules in the original guide. Here are the ten that matter most for cleared candidates today.

01	Clearance at the top. Next to your name. The single most valuable line of text on the document for cleared hiring.
02	Two pages max. Limit to the last 10 years unless niche or executive. Recruiters won't read more.
03	Quantify your impact. Numbers, percentages, dollars, time. "Reduced X by Y%" beats every adjective.
04	Strong action verbs only. Implemented, designed, led, optimized. Skip overused ones like "spearheaded."
05	Tailor for every role. Mirror the job description's language. Move relevant experience to the top.
06	Send as PDF. Preserves formatting. Save as FirstName_LastName_Resume.pdf.
07	Match LinkedIn to resume. Mismatches are a major recruiter red flag. Update both together.
08	Be honest about gaps. Brief acknowledgment is enough. "Career break for caregiving" works.
09	Skip the fluff section. Drop "Key Skills," "Objective," "References Available Upon Request."
10	Proofread relentlessly. Typos cost interviews. Run spellcheck, read aloud, peer review.

ABOUT THIS GUIDE

Informational baseline only. Tier One offers free resume reviews and revisions for cleared candidates — reach out anytime. **Related:** Security Clearances, Compensation Playbook, Cleared Pro Resources.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting
Veteran-Owned | Cleared | Federal Specialists
910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

CLEARED PRO RESOURCES

A Curated Tools Library for Cleared Professionals

UPDATED MAY 2026 • VERSION 2.0

A handpicked library of the tools, platforms, and programs that actually help cleared professionals build careers. **Most are free.** Paid options noted where worthwhile. Got a suggestion? Send it our way and we'll grow the list together.

WHAT YOU'LL FIND IN THIS GUIDE

- **Cleared Job Boards & Career Platforms** Where to look beyond LinkedIn, and the cleared-specific platforms recruiters actually use.
- **Training, Certifications & Clearance Tools** Free training that actually moves the needle, plus the official DCSA tools for managing your clearance.
- **Compensation, Networking & Transition Resources** Salary calculators, professional associations, and dedicated transition programs for service members.
- **Mental Health, News & Writing Tools** Free veteran-focused mental health support, the news sources cleared pros actually read, and resume tools worth using.

CONTENTS

01	Cleared Job Boards & Career Platforms	Page 2
02	Free Training & Certifications	Page 2
03	Clearance Self-Help & Support Tools	Page 3
04	Compensation & Salary Tools	Page 3
05	Networking & Professional Development	Page 3
06	Transitioning Military Resources	Page 4
07	Mental Health & Wellness Support	Page 4
08	News & Resume Tools	Page 4

01 • CLEARED JOB BOARDS & CAREER PLATFORMS

The platforms cleared recruiters and hiring managers actually use. Start with the dedicated cleared boards; supplement with general job platforms for broader reach.

Cleared-Specific (Start Here)

- **ClearanceJobs** — The dominant cleared platform. Recruiters live here.
- **ClearedJobs.Net** — Cleared-only job listings and career resources.
- **IntelligenceCareers.gov** — Official U.S. IC job portal across agencies.
- **Cleared Connections** — Cleared roles in defense and intelligence sectors.
- **Patriot Jobs** — Veteran and cleared roles, defense and government.
- **Silent Professionals** — Private security and cleared defense contracting.

General Platforms (Use the “Security Clearance” Filter)

- **LinkedIn** — Profile + recruiter outreach; essential for visibility.
- **USAJobs** — Federal civilian career portal — the government's own.
- **Indeed / Glassdoor** — Broad reach; use clearance-specific search terms.
- **Dice** — Tech-focused; many cleared IT and cyber roles.
- **MilitaryHire / RecruitMilitary** — Transitioning service members and veterans.
- **CyberSecJobs.com** — Cybersecurity-specific, many cleared listings.

02 • FREE TRAINING & CERTIFICATIONS

Hundreds of hours of free, high-quality training are available to cleared professionals — especially veterans. These are the most useful resources for building skills without spending.

- **FedVTE** — 800+ hours of free cybersecurity training for federal employees and veterans (CISA).
- **DCSA Training** — Courses on personnel security, FSO duties, insider threat.
- **TryHackMe / HackTheBox** — Hands-on cybersecurity labs (free tiers available).
- **IBM Skills Network** — Free training in data science, AI, cybersecurity — certs upon completion.
- **AWS Skill Builder** — Free foundational AWS cloud training.
- **Microsoft Learn** — Free training on Azure, M365, Power Platform.
- **Google Digital Garage** — Free courses in data analysis, cloud, career skills.
- **Coursera / edX (audit)** — University-level IT and cyber courses (audit free; cert paid).
- **Linux Foundation Training** — Open-source and Linux fundamentals.
- **RangeForce / Cybrary** — Cyber defense training (free community tiers).

03 • CLEARANCE SELF-HELP & SUPPORT TOOLS

If you have a clearance, these are the authoritative resources for understanding the process, managing your status, and navigating issues.

- **DCSA (dcsa.mil)** — The single source of truth for federal personnel vetting policy and process.
- **Adjudicative Desk Reference** — Detailed reference for the 13 Adjudicative Guidelines used in clearance decisions.
- **DCSA Self-Reporting Job Aid** — Step-by-step on SEAD 3 reportable events.
- **ClearanceJobs Blog** — Practical guidance on renewals, appeals, and common clearance issues.
- **NBIS / eApp Portal** — The DCSA system that's replacing DISS for clearance management.
- **Your FSO or SSO** — First call for any clearance question — always.

04 • COMPENSATION & SALARY TOOLS

Negotiation works better with data. These are the tools cleared professionals use to benchmark offers.

- **ClearanceJobs Salary Calculator** — Cleared-specific salary trends by role, location, clearance, and polygraph.
- **2025 Security Clearance Compensation Report** — ClearanceJobs' annual industry-wide salary survey — free download.
- **Glassdoor / Levels.fyi** — Company-specific salary insights and reviews.
- **PayScale** — Compare salaries by role, industry, location, experience.
- **NerdWallet Cost of Living Calculator** — Critical for OCONUS and relocation comparisons.
- **BLS Occupational Outlook** — Government data on wages and growth by occupation.

05 • NETWORKING & PROFESSIONAL DEVELOPMENT

The cleared community runs on relationships. These are the highest-leverage networking channels and associations.

Free / Low Cost

- **Cleared & Confused (LinkedIn)** — Tier One's group — open roles, advice, community.
- **LinkedIn Groups** — Search “cleared,” “govcon,” specific agencies, or cert names.
- **OWASP Chapters** — Free local cybersecurity meetups, secure coding, risk management.
- **GitHub** — Build a public portfolio — increasingly important for IT/cyber roles.
- **Meetup** — Local GovCon, cybersecurity, and IT events in your area.
- **Veterati** — Free mentorship platform for transitioning professionals.

Paid Memberships & Conferences (Worth the Investment)

- **AFCEA** — Government / military / industry IT professional association (~\$50-\$150/yr).
- **ISACA** — IT governance and cybersecurity (~\$135/yr).
- **TechNet Cyber** — Premier government IT and cyber conference (AFCEA).
- **RSA Conference** — The largest commercial cybersecurity event.
- **DEF CON** — The original hacker conference — deep technical, strong community.
- **GovCon Summit / IT Symposium** — Industry leadership and contract awards networking.

06 • TRANSITIONING MILITARY RESOURCES

If you're transitioning out of military service, these programs exist specifically to ease the move into cleared civilian work. Use them — most are free and high-leverage.

- **DoD SkillBridge** — Industry internships during your last 180 days of service. The single highest-leverage transition path.
- **Hiring Our Heroes Fellowship** — Corporate fellowship program (Chamber of Commerce).
- **O2O — Onward to Opportunity** — Free Syracuse University training and certifications.
- **MSSA (Microsoft)** — Software engineering and cloud admin training.
- **FourBlock** — Nationwide career readiness, mentorship, networking.
- **VetsinTech** — Education, employment, entrepreneurship in tech.
- **LinkedIn Premium for Veterans** — Free 1-year premium for transitioning service members.
- **Work for Warriors** — Job placement for Guard, Reservists, veterans.

07 • MENTAL HEALTH & WELLNESS SUPPORT

Cleared work is stressful, often classified, and frequently isolating. These resources exist specifically for the veteran and cleared community.

- **Veterans Crisis Line** — Dial 988, press 1. 24/7 confidential support.
- **VA Mental Health Services** — Comprehensive VA mental health support.
- **Cohen Veterans Network** — Free or low-cost mental health care for vets and families.
- **Give an Hour** — Volunteer mental health professionals offering free care.
- **Military OneSource** — Free counseling and resources for service members and families.
- **Wounded Warrior Project Talk** — Confidential, non-clinical emotional support.
- **Real Warriors Campaign** — Resources for service members and veterans.
- **Headspace for Veterans** — Free mindfulness and meditation tools.

08 • NEWS & RESUME TOOLS

Industry News Worth Reading

- **Federal News Network** — Daily federal operations, policy, workforce news.
- **Breaking Defense** — Defense industry, military technology, policy analysis.
- **Defense News** — Global defense policy and military technology.
- **MeriTalk / Nextgov** — Government IT, cloud, cybersecurity coverage.
- **FCW (Federal Computer Week)** — Federal technology and acquisition.
- **Washington Technology** — Government contractor and integrator news.
- **GovConWire** — Contract awards and GovCon industry trends.
- **ClearanceJobs Blog** — Cleared community trends, salary, hiring.

Resume & Writing Tools

- **Grammarly (Free)** — Grammar, clarity, tone for resumes and cover letters.
- **Hemingway Editor** — Highlights complex sentences for clarity.
- **Canva (Free)** — Visual resumes, LinkedIn banners, design templates.
- **Google Docs** — Free collaborative writing with resume templates.
- **Claude / ChatGPT (Free Tier)** — AI assistance — proofread carefully, always personalize.
- **Tier One Resume Review** — Free, no strings. Reach out anytime.

ABOUT THIS GUIDE

Curated, not exhaustive. Resources change — verify the link and program eligibility before relying on it. Got a suggestion? Send it our way and we'll grow this guide together.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 · sgagliardi@tier1-talent.com · tier1-talent.com