The Ultimate GovCon Survival Guide 2025

Prepared by: Tier One Talent
Support Email: sgagliardi@tier1-talent.com
Support Phone: 910.850.3055
LinkedIn Group: Cleared & Confused

Table of Contents

Government Contracting: Quick Reference Guide

Welcome to Your GovCon Guide from Tier One Talent

At Tier One Talent, we're here to help you navigate the Government Contracting (GovCon) industry with confidence. Whether you're just getting started or looking to deepen your career, we're available to support you with any questions or concerns you may have. This guide is designed as a quick reference to help you understand key terms and make informed choices as you explore different job opportunities.

We also offer free assistance with resume reviews, interview preparation, and guidance specific to the IC and GovCon roles. Our team is committed to helping you find a great career fit. Feel free to reach out to us anytime — we're here to help you succeed at every stage of your journey.

1. Take your time – do not rush into any decisions if you are unsure

2. Ask questions – if you don't understand, ask about it

3. Reach out for help – do not be afraid to ask for assistance

Common Terms:

1. Government Contracting (GovCon): Where private companies work with government agencies under specific contracts or task orders to provide services or products.

2. IDIQ (Indefinite Delivery, Indefinite Quantity): A flexible contract structure allowing the government to assign specific tasks over time as needs change.

3. Task Order (TO): A specific project issued under an IDIQ contract. TOs outline exact requirements, timelines, and budgets for tasks within the larger contract.

4. OY (Option Year): Additional years the government can renew on a contract, providing potential for multi-year job stability.

5. Prime Contractor: The primary company holding the main contract with the government.

6. Subcontractor (Sub): Smaller companies on the contract that are given specific Task Orders & a certain number of positions to fill or work to be performed for the customer. The Prime Contractor chooses which Subs will be on the program – the Subs submit proposals to the Prime to be considered for the contract.

7. Customer or Client: The government agency (e.g., DoD, NGA, DHS) that owns and oversees the contract.

8. Defense Information System for Security (DISS): A system used to track security clearances for personnel.

Key Questions to ask the Recruiter or Company Representative:

1. Compensation and Benefits

- What is the total compensation (salary, bonuses, relocation assistance)?
- What benefits are offered (insurance, retirement, PTO)?
- How is pay scheduled, and are there overtime or shift differentials?

2. Position Details

- Where is the work location? Are there remote, travel, or relocation expectations?
- Is relocation assistance provided?
- What training is required, and is it pass/fail?
- What's the work schedule? Does it rotate?

3. Contract and Customer Information

- Is the company a Prime or a Subcontractor?
- What option year is the contract in?

- Who is the customer agency (e.g., NGA, DIA)?

4. Deployment & Rotation(s)

- Are deployments required, and if so, how long?
- What are the deployment rotations?

5. Security Clearance and Commitment

- Will my SSN be required for this application?
- Is there a non-compete clause on the contract?
- How is the clearance process handled, and does it lock me into the company?

6. Additional Tips

- Prepare Follow-Up Questions: Clarify any responses related to training, schedule, or deployments.
- Document Everything: Keep notes for future reference.
- Check Company Stability: Verify the contract's renewal likelihood to understand role continuity.

Have questions or concerns?

Tier One Talent & Intel Recruiting

Tier1-talent.com

sgagliardi@tier1-talent.com

910.850.3055

Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

✨ The Ultimate Tools & Resources Guide for Cleared Professionals ✨

🎯 A One-Stop-Shop for Tools, Training, Certifications, and Career Advancement 🎯

The Ultimate Cleared Professional Resource Guide: This guide is your starting point for navigating the cleared professional world, bringing together **mostly free resources** (with paid options available) to help you thrive. While it's not a *comprehensive* list, it's a great place to begin building your career and skills. **Got a suggestion? Let us know, and we'll grow the guide together!**

Here's what you'll find:

🔍 Job Boards: Your Gateway to Cleared Opportunities

- **Certifications**: Boost your credentials with industry-recognized certifications.
- **Training Resources**: Free and paid tools to upskill in IT, cybersecurity, cloud, and more.
- **Networking Tools**: Connect with other professionals in the cleared and GovCon community.
- **Mental Health Tools**: Free support to help you maintain balance and well-being.
- **News Resources**: Stay informed with updates on government, defense, and IT trends.

---

1. Job Boards & Career Platforms: These platforms are essential for finding cleared and related roles.

- [ClearanceJobs](): Dedicated platform for security-cleared positions.

- [Cleared Connections](): Offers a range of job listings for individuals with security clearances, focusing on defense and intelligence sectors.

- [ClearedJobs.Net](): Provides job listings and career resources specifically for cleared professionals.

- [Contract Professionals Inc. (CPI)](): Focused on cleared roles in engineering and aerospace.

- [CyberSecJobs.com](): Focuses on cybersecurity positions, including those requiring security clearances.

- [DefenseCareers.com](): Provides job listings in the defense industry, including roles requiring security clearances.

- [Dice](): Tech-specific job board often featuring roles requiring clearances.

- [Glassdoor](): Search jobs while reading reviews about salaries and company culture.

- [GovLoop](): Government-focused networking site with job opportunities and free learning resources.

- [Indeed](): Use search terms like "security clearance" to find relevant roles.

- [IntelligenceCareers](): Jobs in intelligence, DoD, and federal agencies.

- [IntelligenceCareers.gov](): The official job portal for the U.S. Intelligence Community, listing positions that require various levels of security clearance.

- [LinkedIn](): Build a professional profile, highlight your clearance, and connect with recruiters.

- [MilitaryHire](): Job platform for transitioning service members and veterans.

- [Patriot Jobs](): Caters to veterans and cleared professionals seeking employment in defense and government sectors.

- [Security Clearance Careers](): Offers a variety of job listings for individuals with active security clearances.

- [SecurityJobsToday.com](): Features security-related job postings, some of which require clearances.

- [Silent Professionals](): Specializes in private security and defense contracting jobs, including roles requiring security clearances.

- [USAJobs](): Federal government's official job portal.

- [WeWorkRemotely](): Lists remote jobs, including roles in cleared industries.

---

2. Training & Certifications: Certifications & training are key for breaking into and advancing in IT.

- [Alison](): Offers a wide range of free IT courses in networking, security, software development, and more.

- [AWS Skill Builder](): Free foundational courses on AWS cloud computing.

- Class Central: Aggregates over 900 free developer and IT certification courses from various providers.
- CodeAcademy Free Tier: Learn programming languages like Python, SQL, and Java for free.
- Coursera: Offers free courses in IT and data science (select options).
- Cybersecurity and Infrastructure Security Agency (CISA): Webinars, cybersecurity exercises, and tools.
- Defense Counterintelligence and Security Agency (DCSA): Free courses in information and personnel security.
- EC-Council Essentials: Free courses for beginners in cybersecurity.
- edX: Free courses from top universities on IT, networking, and cybersecurity (with an option to pay for certificates).
- Federal Virtual Training Environment (FedVTE): Over 800 hours of free cybersecurity training for federal employees and veterans.
- GCFLearnFree.org: Provides free tutorials on technology, job training, reading, and math skills.
- Google Digital Garage: Free courses in data analysis, cloud computing, and career skills.
- Google IT Automation with Python: Free for limited periods via Coursera's scholarships.
- Harvard Online Courses: Free courses in computer science, cybersecurity, and AI.
- IBM Skills Network: Free training in data science, cybersecurity, and AI, with certifications upon completion.
- LaunchCode: A nonprofit offering free coding bootcamps and training programs to help individuals enter the tech industry.
- Linux Foundation Training: Free courses on Linux, cloud infrastructure technologies, and open-source software development.
- Microsoft Learn: Free training on Microsoft Azure, M365, and more.
- MIT OpenCourseWare: Free IT, engineering, and project management courses from MIT.
- Open Learning for Development: A UNESCO-driven platform offering free training and learning resources on a wide range of development topics.
- Pluralsight Free Weekend: Periodically offers free access to its entire library, including IT and cybersecurity courses.
- RangeForce Community Edition: Free hands-on cyber defense training.
- TryHackMe: Free hands-on cybersecurity training for beginners and professionals.
- U.S. Cyber Range: Free cybersecurity labs and training for military and government personnel.

Common Baseline Certifications (Paid):

- CompTIA A+: Foundation for IT roles ($246 per exam).
- CompTIA Network+: Networking concepts, configuration, and troubleshooting (~$338).
- CompTIA Security+ and/or IAT I, II, III: Entry-level cybersecurity certification (~$392).
- Cisco Certified Network Associate (CCNA): Networking and security fundamentals (~$300).

Advanced Certifications (Paid):

- AWS Certified Solutions Architect – Associate: Validates skills in designing & deploying scalable systems on AWS
- Certified Ethical Hacker (CEH): Focused on ethical hacking and penetration testing
- Certified Information Systems Security Professional (CISSP): Industry-leading credential for cybersecurity leaders
- GIAC Security Essentials (GSEC): Comprehensive foundational cybersecurity certification
- Google Professional Cloud Architect: Validates expertise in advanced cloud architecture design

- ITIL 4 Foundation: Focused on IT service management best practices
- Offensive Security Certified Professional (OSCP): Advanced certification for ethical hacking and penetration testing
- Project Management Professional (PMP): Gold standard for project management certification

3. Clearance Management & Support:

- Adjudicative Desk Reference (ADR): Provides detailed information on clearance adjudication factors to help professionals understand denials and appeals.
- Adjudicative Guidelines: Explains how clearance decisions are made, enabling management of your standing.
- Clearance Self-Check Guide (DCSA): A step-by-step guide to managing clearance issues effectively.
- ClearanceJobs Blog: Offers expert advice on navigating clearance renewals, appeals, and common issues.
- Defense Counterintelligence and Security Agency (DCSA): Official portal for managing clearance renewals and updates, as well as understanding clearance-related processes.

💡 Additional Guidance

- If you have questions or need support regarding your clearance, always reach out to your SSO (Special Security Officer) or FSO (Facility Security Officer) for tailored advice and assistance. They are your primary resource for clearance-related matters.

4. Networking & Professional Development:

- Cleared Connections: A networking site specifically designed for cleared job seekers.
- Eventbrite: Find free local events for GovCon, IT, and networking opportunities.
- GitHub: A platform for developers to showcase projects, contribute to open-source communities, and connect with peers.
- LinkedIn Groups: Join groups like "Cleared Professionals Network" or "GovCon Talent Network" to expand your professional connections.
- Meetup: Search for local GovCon, cybersecurity, and IT-related networking events in your area.
- OWASP: Participate in free global meetups focused on cybersecurity, secure coding practices, and risk management.
- Security Clearance Careers (GovCon Careers): Connect with recruiters actively hiring for cleared roles in defense and intelligence.
- Veterati: A free mentorship platform tailored for transitioning professionals seeking guidance and career advice.

Paid Opportunities:

- AFCEA Membership: A professional association connecting individuals in government, military, and industry IT. Provides access to events, resources, and valuable networking opportunities (~$50-$150/year).
- Black Hat Conferences: Industry-leading events for cybersecurity professionals to network, share knowledge, and learn about cutting-edge security technologies (~$2,500+ per ticket).
- DEF CON: One of the largest and oldest hacker conferences, offering unparalleled networking opportunities for cybersecurity professionals (~$300+).
- Gartner IT Symposium/Xpo: A leading IT conference for government and industry professionals focused on innovation, strategy, and networking (~$4,000+).
- GovCon Summit: Paid networking events bringing together leaders in the government contracting (GovCon) industry to share insights and make valuable connections.
- ISACA Membership: Offers access to IT governance and cybersecurity certifications, training, and networking events (~$135/year).

- RSA Conference: A premier cybersecurity event featuring networking opportunities, workshops, and exhibitions (~$1,500+).
- TechNet Cyber: A high-profile networking event focused on government IT and cybersecurity professionals, hosted by AFCEA (~$1,000+

5. Salary & Benefits Tools:

- ClearanceJobs Salary Calculator: Provides tailored salary estimates specifically for roles requiring security clearances.
- Glassdoor: Offers company reviews, salary insights, and information on benefits from current and former employees.
- NerdWallet Cost of Living Calculator: Compare the cost of living between locations to evaluate job offers effectively.
- PayScale: Allows you to compare salaries by role, industry, location, and experience level.

Paid Resources:

- Salary.com Premium: In-depth salary reports ($29.95/month).
- Payscale Career Profile: Comprehensive salary benchmarking for cleared roles (~$29.99/month).

6. Mental Health & Wellness:

- BetterHelp for Veterans: Offers discounted online therapy services tailored for veterans and their families.
- Cohen Veterans Network: Provides free or low-cost mental health care specifically designed for veterans and their families.
- Give an Hour: Connects military personnel, veterans, and their families with volunteer mental health professionals offering free care.
- Headspace for Veterans: Provides free mindfulness and meditation tools to enhance mental well-being for veterans.
- Make the Connection: Features real stories from veterans and provides resources for overcoming mental health challenges.
- Military OneSource: Offers free counseling services, resources, and support for service members, veterans, and their families.
- National Veterans Crisis Line: Provides 24/7 confidential support for veterans, active-duty members, and their families.
- Real Warriors Campaign: Offers resources and support to address mental health challenges faced by service members and veterans.
- VA Mental Health Services: Provides comprehensive mental health services through the Department of Veterans Affairs.
- Wounded Warrior Project (WWP) Talk Program: Offers confidential, non-clinical emotional support and assistance for warriors and their families.

7. Transitioning Military Resources:

Career Transition & Job Placement

- DoD SkillBridge: Provides internships and certifications during the last 180 days of service to prepare for civilian careers.
- HireMilitary: Free job placement services connecting transitioning personnel with employers seeking military talent.

- Veteran and Military Transition Center: A one-stop site for employment, training, and financial resources for veterans and transitioning service members.
- RecruitMilitary: Connects veterans and service members with job fairs, career opportunities, and resume assistance nationwide.
- LinkedIn Premium for Veterans: Free one-year premium account for transitioning service members to network and find job opportunities.
- FourBlock: A nationwide career readiness program providing workshops, mentorship, and networking opportunities.
- O2O - Onward to Opportunity: A free career training and certification program through Syracuse University.
- Amazon Military Programs: Career opportunities for transitioning service members in IT, logistics, and operations.
- Work for Warriors: Job placement services for National Guard, Reservists, and veterans.
- Corporate Fellowship Program (Hiring Our Heroes): Offers professional training and hands-on experience in civilian careers.
- Helmets to Hardhats: Connects transitioning service members to apprenticeship opportunities in construction and related industries.

Financial, Education, & Family Support

- GI Bill Comparison Tool: Helps maximize education benefits and understand tuition assistance options.
- Work Opportunity Tax Credit (WOTC): Provides tax incentives for employers hiring veterans and transitioning service members.
- Military OneSource Transition Assistance Programs: Comprehensive resources for service members and their families navigating the transition to civilian life.
- Patriot Boot Camp: Helps veterans and military spouses start businesses through mentorship and training.
- Operation Homefront: Offers financial planning, housing assistance, and family support.

Training & Internships

- Microsoft Software & Systems Academy (MSSA): Provides training in software engineering and cloud administration for transitioning service members.
- SkillMil: Offers SkillBridge internships tailored to align military skills with civilian opportunities.
- VetsinTech: Connects veterans to tech industry resources in education, employment, and entrepreneurship.
- Northrop Grumman Military Internship Program: Offers internships in defense and aerospace through the SkillBridge program.
- Apprenti: Provides registered apprenticeship programs in technology roles, combining paid on-the-job training and education.
- Per Scholas: Tuition-free training in IT and software engineering with career placement support.
- Revature: Offers training and placement in software engineering roles.
- Cisco Veteran Talent Incubation Program: Provides training and employment opportunities in technology careers.

---

8. Writing & Resume Tools:

- Canva Free: Design visually appealing resumes, LinkedIn banners, and other professional documents.
- ChatGPT (Free Tier): AI for drafting resumes, brainstorming ideas, and refining professional content.
- Copy.ai: AI-powered tool for generating copy for resumes, LinkedIn summaries, and cover letters. *(Free plan available)*
- DeepAI: Free AI tools for generating creative content and exploring AI-based text solutions.

- **Google Docs**: Collaborative writing platform with free templates for resumes, cover letters, and more.
- **Grammarly Free**: Improve grammar, clarity, and tone in resumes, cover letters, and emails.
- **Hemingway Editor**: Highlights complex sentences and errors to improve clarity and readability.
- **Hugging Face**: Access pre-trained AI models for natural language processing tasks.
- **Jasper AI**: AI-powered writing assistant for creating polished, professional content. *(Free trial available)*
- Microsoft Word Online: Create and format professional documents for free using Microsoft's web-based editor.
- **OpenAI Playground**: Experiment with GPT models for content generation and conversational AI.
- **ProWritingAid Free**: Advanced grammar and style editor for improving overall writing quality.
- **Resumake.io**: Generate professional resumes tailored to specific industries.
- Zety Resume Builder: Offers AI-driven resume building and formatting tools. *(Free basic features)*

9. Industry News & Updates:

- **Acquisition.gov News**: Provides official news and announcements related to federal acquisition regulations and policies.
- **Breaking Defense**: Focuses on defense industry news, military technology, and policy analysis.
- **Defense News**: Covers defense policies, military technology, and global security news.
- **ExecutiveBiz**: Provides news on government contracting companies, focusing on executive-level business activity and corporate developments.
- **ExecutiveGov**: Offers news and insights on government policies, executive movements, and federal government developments.
- **FCW (Federal Computer Week)**: Specializes in federal technology and business management news.
- **Federal News Network**: Delivers updates on government operations, policies, and federal workforce news.
- **Federal Times**: Focuses on federal procurement, policy, and management for federal managers and executives.
- **Fedscoop**: Provides the latest news on federal IT, policy, and modernization efforts.
- **GovConWire**: Offers insights on government contracting trends, major contract awards, and industry developments.
- **Government Executive**: Delivers news and analysis on federal management, policy, and politics.
- **MeriTalk**: Covers government IT, cloud computing, and cybersecurity news.
- **Nextgov**: Focuses on IT modernization, emerging technologies, and cybersecurity news within federal agencies.
- **PubKGroup**: Offers comprehensive news on government contracting, law, cybersecurity, and compliance.
- **Washington Technology**: Provides news and insights for government contractors and the integrator community.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

The No-BS Resume Guide 2025

This guide serves as a baseline for crafting civilian resumes in the government contracting world but is not a one-size-fits-all solution. Resumes should always be tailored to your specific industry, job, and role, as each sector has unique standards. For example, federal resumes follow entirely different guidelines than those outlined here. Use this guidance as a starting point, and if you're unsure how to proceed, don't hesitate to seek additional help or clarification.

---

1. Contact Information—What Belongs and What Doesn't: Your contact details should be unmissable and professional, right at the top.

What to include:
- ✓ **Name**: Big and bold, followed by your clearance level if applicable.
  - ▪ Example: **Jane Doe | TS/SCI/FSP Clearance**
- ✓ **Location**: Just the city and state (e.g., Washington, D.C.).
- ✓ **Phone number**: Mobile only.
- ✓ **Professional email**: Think professional; not hotbunz69@gmail.com.
- ✓ **LinkedIn (optional)**: If it's listed, make sure it's up-to-date and polished. Make sure your LinkedIn profile and your resume match – this is a major red flag if there are discrepancies.

What NOT to include:
- X DOB | SSN | Full address | Hobbies | "References available upon request | Pictures |

---

2. Formatting Rules Everyone Needs to Follow: Keep your resume simple, clean, and professional.

- ✓ Use easy-to-read fonts like Calibri, Arial, or Times New Roman (10-12 pt).
- ✓ Present tense for your current role, past tense for all others.
- ✓ Check your grammar and spelling. Typos can cost you the job.
- ✓ Bullet points > paragraphs. Recruiters & Hiring Managers don't read essays.
- ✓ Check your spacing – do not overcrowd your resume.
- ✓ Use "narrow" margins for more room if needed.
- ✓ You can be creative with the layout – but keep it clean and simple – white space is good!
- ✓ Save & send your resume as a PDF unless otherwise directed.

---

3. Nail the Summary Section: No need to label this section as "Professional Summary"—just dive in. Every inch of your resume matters, so make it count.

- Keep it concise: 2–5 tailored sentences maximum.
- Focus on your key skills, experience, and the value you bring to the role.
- Avoid generic terms or blanket statements; make your introduction unique and memorable.
- Minimize "I" statements to maintain a professional tone.
- Write in a first-person perspective (not third person) to create a more genuine and personal connection.

Example: "IT professional with 8+ years of experience in designing and managing secure, enterprise-level networks. Expertise in optimizing infrastructure for 99.9% uptime, implementing advanced cloud architectures, and delivering scalable solutions. Holds active TS/SCI/FSP clearance and a strong track record of driving efficiency and innovation in mission-critical environments."

---

4. Order and Structure Matter: Here's the ideal layout for your resume.

1. **Contact Info** (top).

2. **Summary** (no label).

3. **Certifications & Skills (if relevant to the field).**

4. **Experience** (most recent role first):

   ▪ Title | Company | Location | Dates (Month/Year).

   ▪ 5+ impactful bullet points per role minimum – more if you have a lot of blank space.

5. **Education** (degrees separated by "|" instead of commas)

6. **If you have extra room, consider adding a meaningful section. See #10 below.**

---

5. Certifications & Skills—Prioritize for IT/Technical Roles: For IT and technical fields, list your certifications, degrees, and tech skills **right under the summary** to grab attention immediately.
Break up the Certifications & Skills – make it easy to read.
Example:

Certifications:

- **Cybersecurity**: CISSP, CISM, CEH, CompTIA Security+, GCIH, GPEN
- **Cloud**: AWS Certified Solutions Architect, Azure Solutions Architect Expert, Google Cloud Professional
- **Networking**: CCNA, CCNP, CompTIA Network+, Palo Alto PCNSA/PCNSE
- **Project Management**: PMP, ITIL Foundation, Scrum Master (CSM, PSM)
- **Operating Systems**: Microsoft Certified: Azure Administrator Associate, Red Hat Certified Engineer (RHCE)
- Data & Databases: Microsoft Certified: Data Analyst Associate, Oracle Certified Professional
- Other IT Skills: CompTIA A+, TOGAF, Linux+

Technical Skills:

- **Network Administration:** Routing & switching, firewalls, VPNs, DNS, DHCP, VLANs
- **Cybersecurity:** Vulnerability assessment, penetration testing, SIEM, incident response, IDS/IPS
- **Cloud Computing:** AWS, Azure, Google Cloud, hybrid and multi-cloud architectures
- **Programming & Scripting:** Python, PowerShell, Bash, JavaScript, SQL, JSON
- **Data Management:** Database administration, ETL processes, data analytics, big data tools
- **DevOps:** CI/CD pipelines, containerization (Docker, Kubernetes), Jenkins, Ansible, Terraform
- **IT Support:** Helpdesk management, hardware/software troubleshooting, ticketing systems
- **System Automation:** Automation scripts, RPA tools, workflow optimization

---

Systems & Tools:

- **Operating Systems:** Windows Server, Linux (Ubuntu, Red Hat, CentOS), macOS
- **Virtualization:** VMware vSphere, Hyper-V, Citrix
- **Cloud Platforms:** AWS (EC2, S3, RDS), Azure (Active Directory, Virtual Machines), GCP
- **Security Tools:** Nessus, Splunk, Wireshark, Metasploit, Kali Linux, CrowdStrike, Palo Alto, Cisco ASA
- **Monitoring Tools:** Nagios, SolarWinds, Zabbix, Datadog
- **Version Control:** Git, GitHub, GitLab
- **Database Management:** MySQL, PostgreSQL, Oracle DB, MongoDB
- **ITSM Tools:** ServiceNow, Jira, Confluence
- **Collaboration Tools:** Slack, Microsoft Teams, Zoom
- **Automation Tools:** Puppet, Chef, Ansible, Terraform

For other industries, keep education and certifications toward the bottom.

---

6. Bullet Points That Actually Mean Something: Skip the fluffy, meaningless phrases and focus on specifics.

- **Wrong**: "Effectively communicated with team members to achieve goals."
- **Right**: "Led a cross-functional team of 10 to deliver a $1.2M project two weeks ahead of schedule."

Bullet consistency: Use the same style and indentation for all bullet points (e.g., circles, dashes, or solid dots).

Formula for strong bullet points: Action Verb + Task/Responsibility + Impact/Result

---

7. Tailor Your Resume to the Job and Industry: No generic resumes. Narrow it down to your target industry and customize it.

- ✓ Research common keywords and skills for that industry.
- ✓ Align your achievements with what the company is looking for.

Pro Tip: Once you've nailed your industry-specific resume, tailoring it for individual jobs gets much easier.

---

8. Career Gaps: Be Honest, Keep It Brief: Recruiters appreciate honesty, not oversharing.

Example: "2021–2022: Career break for caregiving responsibilities."
That's it. No need to write an essay. Acknowledge it and move on.

---

9. Recruiters Check Everything—Don't Lie or Embellish: Inflating your achievements might get you an interview, but it can cost you the job and your reputation!

- ✓ If you use AI tools like ChatGPT to refine your resume, **proofread and fact-check** before submitting.

---

10. Remove the "Key Skills" Section – It's Vague & Outdated: The old "Key Skills" section (e.g., a list of generic buzzwords like "teamwork" or "problem-solving") is a waste of valuable space. Instead, replace it with something meaningful.

Options:

1. **Certifications and Technical Skills (for IT/Technical Roles):**
   List relevant certifications and technical proficiencies right under your summary.
   Example:
   - ✓ Certifications: AWS Certified Solutions Architect | CISSP | CompTIA Security+
   - ✓ Skills: Python | Kubernetes | Cloud Migration | CI/CD Pipelines

2. **Career Highlights (for Senior/Leadership Roles):** A brief list of measurable achievements to hook the reader.
   Example:
   - ✓ Delivered $2M cost savings by streamlining supply chain processes.
   - ✓ Led a global marketing campaign that increased ROI by 25%.

3. **Core Competencies (for General Roles):** A compact list of your expertise areas tailored to the role.
   Example:
   - ✓ Strategic Planning | Budget Management | Data Analytics | Process Improvement

4. **Project List: Project Name | Role | Date**
   Example:
   - ✓ Hybrid Cloud Infrastructure Migration: Designed and executed migration strategy for on-prem systems to AWS, ensuring 100% data integrity.
   - ✓ Zero-Trust Security Implementation: Deployed zero-trust architecture across 5 global offices, enhancing security compliance.

The No-BS Golden Rules for Your Resume

Structure and Formatting:

1. **Keep It Concise:** Limit your resume to two pages, unless applying for executive or niche roles. Focus on the last 10 years of experience to keep it relevant.

2. **Use a Clean, Consistent Format:** Choose professional fonts (e.g., Calibri, Arial, Times New Roman), avoid overcrowding, and balance white space for readability.

3. **Always Send as a PDF:** Save and send your resume as a PDF unless another format is specifically requested.

4. **Test for Readability Across Devices:** Make sure your resume looks professional on both desktop and mobile screens.

5. **Make Contact Info Obvious:** Include your name, phone number, email, city, and LinkedIn profile (if professional).

Content and Customization:

6. **Tailor Your Resume for Each Role:** Use industry-specific keywords and align your skills and experience with the job description.

7. **Avoid Copy-Pasting Job Descriptions:** Write authentically; recruiters will notice if it's copied—even with "hidden" text tricks.

8. **Quantify Results Over Listing Responsibilities:** Focus on measurable achievements (e.g., "Reduced downtime by 30%") to demonstrate impact.

9. **Current Role = Present Tense; Past Roles = Past Tense:** Ensure grammatical consistency throughout your resume.

10. **Highlight Certifications and Skills Where Relevant:** For IT/technical roles, list them at the top. For others, include them at the bottom.

11. **No Fluff Words:** Avoid clichés like "team player" or "hard worker" unless backed up with concrete examples.

12. **Provide Relevant Links:** Include links to your LinkedIn, portfolio, GitHub (for IT roles), or professional website, if applicable.

Content Organization:

13. **Use Strong Action Verbs:** Start bullet points with impactful words like "Implemented," "Optimized," or "Designed," and avoid overused terms like "spearheaded."

14. **Use Metrics Wisely:** Include numbers, percentages, or measurable outcomes, but don't overwhelm the reader.

15. **Include a Career Highlights Section (for Senior Roles):** Showcase 2-4 standout accomplishments upfront for quick impact.

16. **Five Strong Bullet Points Per Job Minimum:** Each point should focus on action and results.

17. **Keep Technical Skills Separate:** Add a dedicated section for tools, technologies, and certifications, especially for IT or technical roles.

Professionalism and Compliance:

18. **Ensure LinkedIn Matches Your Resume:** Inconsistent profiles are a red flag for recruiters.

19. **List Clearance at the Top:** If applicable, place your clearance designation (e.g., TS/SCI/FSP) prominently near your name.

20. **Stay Professional:** Use a polished email address and save your file with a clear name (e.g., FirstName_LastName_Resume.pdf).

21. **Keep Personal Details Off:** Do not include photos, hobbies, full address, date of birth, or social security number.

Final Touches:

22. **Avoid "References Available Upon Request:"** It's outdated and unnecessary—everyone assumes this.

23. **Skip Headers Like "Professional Summary" if Space Is Tight:** Just dive into your content.

24. **Use "|" to Save Space:** Separate degrees, certifications, or skills with "|" to keep it clean and concise.

25. **Optimize for ATS:** Use keywords naturally, avoid images or complex formatting, and keep the layout ATS-friendly.

26. **Proofread Relentlessly:** Spellcheck, check for typos, and ensure grammatical accuracy. Ask trusted colleagues for feedback.

27. **Take Advice That Works for You:** Use these rules as a guide but adapt based on your unique goals and career needs.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

John Doe | Cybersecurity Engineer | Clearance: TS/SCI/FSP

Washington, D.C. | j.doe@gmail.com | 555-555-5555 | linkedin.com/in/johndoe

Experienced cybersecurity professional with 10+ years of proven success in protecting enterprise systems and ensuring compliance with federal standards. Skilled in designing and managing secure infrastructures, mitigating threats and optimizing cloud security solutions. Reduced vulnerabilities by 40% across high-risk platforms while maintaining 99.9% uptime for mission-critical systems.

Certifications and Technical Proficiencies:

Certifications:

- CompTIA Security + | Network+ | CCNA | CCNP | GSEC

Technical Skills:

- **Network Administration:** Routing & switching, firewalls, VPNs, DNS, DHCP, VLANs
- **Cybersecurity:** Vulnerability assessment, penetration testing, SIEM, incident response, IDS/IPS
- **Cloud Computing:** AWS, Azure, Google Cloud, hybrid and multi-cloud architectures
- **Programming & Scripting:** Python, PowerShell, Bash, JavaScript, SQL, JSON
- **Data Management:** Database administration, ETL processes, data analytics, big data tools
- **DevOps:** CI/CD pipelines, containerization (Docker, Kubernetes), Jenkins, Ansible, Terraform
- **IT Support:** Helpdesk management, hardware/software troubleshooting, ticketing systems
- **System Automation:** Automation scripts, RPA tools, workflow optimization

Systems & Tools:

- **Operating Systems:** Windows Server, Linux (Ubuntu, Red Hat, CentOS), macOS
- **Virtualization:** VMware vSphere, Hyper-V, Citrix
- **Cloud Platforms:** AWS (EC2, S3, RDS), Azure (Active Directory, Virtual Machines), GCP
- **Security Tools:** Nessus, Splunk, Wireshark, Metasploit, Kali Linux, CrowdStrike, Palo Alto, Cisco ASA
- **Monitoring Tools:** Nagios, SolarWinds, Zabbix, Datadog
- **Version Control:** Git, GitHub, GitLab
- **Database Management:** MySQL, PostgreSQL, Oracle DB, MongoDB
- **ITSM Tools:** ServiceNow, Jira, Confluence
- **Collaboration Tools:** Slack, Microsoft Teams, Zoom
- **Automation Tools:** Puppet, Chef, Ansible, Terraform

Career Highlights:

- Secured a $5M federal contract by leading the development of a compliance-driven cybersecurity strategy, meeting all NIST 800-171 requirements ahead of schedule.

- Designed and implemented a company-wide incident response plan that successfully mitigated a ransomware attack, preventing potential data loss across critical systems.

- Recognized with the "Innovator of the Year" award for introducing an automated vulnerability scanning tool that improved detection accuracy and reduced manual effort by 50%.

Professional Experience:

Senior Cybersecurity Engineer | SecureTech Solutions | Arlington, VA | Jan 2018 – Present

- Implement a zero-trust security framework, improving overall system security and reducing unauthorized access incidents by 25%.

- Deploy SIEM solutions (Splunk, QRadar) to streamline threat detection and enhance incident response times by 40%.

- Conduct risk assessments with internal teams to address vulnerabilities and ensure compliance with NIST 800-53 and FISMA standards.
- Collaborate with IT leadership to align security measures with organizational goals, supporting cloud migration initiatives for hybrid environments.
- Mentor and train a team of 10+ junior analysts, fostering skill development and improving team performance by 30%.

Cybersecurity Analyst | GovProtect Inc. | Washington, D.C. | May 2014 – Dec 2017

- Monitored network activity to identify and mitigate cybersecurity threats, reducing vulnerabilities by 20% through proactive risk management.
- Deployed encryption protocols for federal clients, ensuring full compliance with federal data security mandates.
- Led a collaborative effort to upgrade legacy systems, improving system resilience and operational efficiency.
- Authored detailed incident response reports for executive leadership, enabling informed decision-making during security events.
- Developed and maintained a vulnerability remediation schedule, reducing downtime caused by patching activities.

IT Support Specialist | TechNova Corp. | Bethesda, MD | June 2012 – April 2014

- Provided tier-3 support for network and system issues, maintaining a 90% resolution rate within SLA timeframes.
- Assisted in the migration of legacy systems to a cloud-based infrastructure, streamlining operations and reducing costs by 15%.
- Managed inventory and procurement of IT hardware and software, ensuring seamless operation across teams.
- Conducted system backups and implemented disaster recovery plans, minimizing potential downtime during outages.
- Delivered hands-on training sessions for employees, improving adoption rates of new software tools by 30%.
- Designed and documented internal knowledge base articles to standardize troubleshooting processes across the IT department.

Relevant Projects:

- **Hybrid Cloud Infrastructure Migration:** Designed and executed migration strategy for on-prem systems to AWS, ensuring 100% data integrity.
- **Zero-Trust Security Implementation:** Deployed zero-trust architecture across 5 global offices, enhancing security compliance.
- **DevOps Pipeline Automation:** Built an end-to-end CI/CD pipeline using Jenkins, Docker, and Kubernetes, improving deployment efficiency.

Education:

▪ BS Cybersecurity | University of Maryland
▪ AAS Information Technology | University of Maryland

Comprehensive Guide to Security Clearances

1. Security Clearance Basics:

- **Purpose**: Security clearances allow individuals to access classified information critical to national security. They are required for many federal, DoD, intelligence, and government contractor roles.

- **Clearance Levels**:
  - ✓ **Confidential (Tier 1)**: Minimal damage if disclosed.
  - ✓ **Secret (Tier 3)**: Serious damage if disclosed.
  - ✓ **Top Secret (Tier 5)**: Exceptionally grave damage if disclosed.
  - ✓ **SCI (Sensitive Compartmented Information)** and **SAP (Special Access Programs)**: Special designations at the Top-Secret level for highly compartmentalized information.
  - ✓ **DOE Clearances**: "Q" (like Top Secret) and "L" (like Secret) for nuclear and energy roles.

2. Key Agencies and Their Roles:

- **Defense Counterintelligence and Security Agency (DCSA)**: Conducts background investigations for DoD and many federal agencies.

- **Department of Defense Consolidated Adjudications Facility (DoD CAF)**: Reviews investigation results and makes clearance eligibility decisions for DoD personnel.

- **Intelligence Community Agencies (CIA, NSA, FBI)**: Conduct their own investigations and grant clearances tailored to intelligence needs.

- **Department of Energy (DOE)**: Manages Q and L clearances for nuclear information.

- **Department of State**: Grants clearances for roles involving diplomatic and foreign relations.

3. Security Clearance Process:

- **Application**: Initiated by the sponsoring agency or employer, often requiring completion of Standard Form 86 (SF-86).

- **Background Investigation**:
  - ✓ Conducted by DCSA or agency-specific investigators. Involves credit checks, criminal record reviews, interviews, and verification of foreign contacts and financial stability.

- **Adjudication**:
  - ✓ The adjudicating agency (DoD CAF, CIA, FBI, etc.) reviews findings against the **13 Adjudicative Guidelines**, which include foreign influence, financial considerations, personal conduct, and more.

4. Continuous Evaluation (CE)

- **Purpose**: CE is a real-time, ongoing monitoring process for individuals with clearances.

- **Functionality**: CE includes checks on credit, criminal records, and other public records to identify potential security risks before they escalate.

- **System Integration**: CE is supported by DISS and NBIS, ensuring agencies stay updated on any changes in an individual's risk factors.

5. The "13 Adjudicative Guidelines:"

- The guidelines include factors such as **Allegiance to the United States**, **Foreign Influence**, **Sexual Behavior**, **Financial Considerations**, **Criminal Conduct**, and others.

- Adjudicators use these guidelines to evaluate the "whole person" and make decisions on eligibility based on national security considerations.

6. Common Reasons for Denial or Revocation:
- Security clearance denials often stem from:
  - ✓ **Financial issues** (e.g., high debt, unresolved bankruptcies).
  - ✓ **Criminal conduct** (e.g., recent arrests, drug involvement).
  - ✓ **Foreign contacts** (e.g., connections that could pose a security risk).
  - ✓ **Personal misconduct** (e.g., false information, mishandling classified information).

7. Maintaining and Renewing a Security Clearance:
- **Reinvestigations**:
  - ✓ **Confidential**: Every 15 years.
  - ✓ **Secret**: Every 10 years.
  - ✓ **Top Secret**: Every 5 years (or ongoing CE).
- **Reporting Requirements**: Cleared personnel must report significant life changes, arrests, or changes in foreign contacts.

8. Key Clearance Management Systems:
- **Defense Information System for Security (DISS)**: Manages and verifies DoD clearances.
- **Scattered Castles**: Used by Intelligence Community agencies to track and verify clearances for IC personnel.
- **National Background Investigation Services (NBIS)**: New DoD system that integrates clearance management, CE, and investigation tracking.
- **Continuous Evaluation Systems**: CE programs integrated into DISS and NBIS provide real-time risk assessment.

9. DHS and Other Agencies' Clearances:
- **DHS Clearances**: DHS grants standard federal clearances (Confidential, Secret, Top Secret) for roles in homeland security, law enforcement, and cybersecurity.
- **Reciprocity Across Agencies**: Federal guidelines generally support reciprocity, allowing agencies to recognize clearances from other agencies. Additional checks or agency-specific requirements (such as polygraphs for CIA/FBI or DHS suitability reviews) may still be required.

10. Compatibility and Transfers Between Agencies:
- **Reciprocity**: Clearances are often transferable between agencies through reciprocity agreements, but additional steps may be needed for SCI, SAP, or roles requiring polygraphs.
- **Agency-Specific Checks**: While a DHS clearance may be transferable to DoD, the new agency might perform additional checks or require enrollment in its Continuous Evaluation program.
- **Special Access Requirements**: Some intelligence roles may require re-adjudication or new background investigations due to agency-specific guidelines.

Investigation Type	Standard Cost
National Agency Check (NAC)	$140
Tier 1 (Non-Sensitive Low Risk)	$180
Tier 2 (Moderate Risk Public Trust)	$420
Tier 2R (Reinvestigation)	$380
Tier 3 (Non-Critical Sensitive – Secret)	$420
Tier 3R (Reinvestigation)	$380
Tier 4 (High Risk Public Trust)	$4,095
Tier 4R (Reinvestigation)	$2,530
Tier 5 (Critical and Special Sensitive – Top Secret and SCI)	$5,410
Tier 5R (Reinvestigation)	$2,965

Quick Reference Guide: SF-86 and Continuous Evaluation (CE)

SF-86 Overview:

- **Purpose**: Used to conduct background checks for security clearance eligibility and reinvestigations.
- **Information Included**: Personal history, employment, education, foreign contacts, financial status, criminal history, etc.
- **Who Uses It**: Required for anyone applying for or renewing a security clearance, particularly for Secret, Top Secret (TS), and Sensitive Compartmented Information (SCI) levels.

When SF-86 is Required:

1. **Initial Clearance Application**: Required for anyone applying for a clearance for the first time.
2. **Periodic Reinvestigations (PRs)**:
   - ✓ **TS/SCI**: Every **6 years** (previously 5 years).
   - ✓ **Secret**: Every **10 years**.
3. **Upgrading Clearance Level**: Required if upgrading from Secret to TS or SCI.
4. **Break in Service**: If clearance is inactive (no sponsorship) for over 2 years, a new SF-86 is needed.
5. **Triggered Reinvestigations**: Additional SF-86 may be requested if Continuous Evaluation flags potential issues.

Continuous Evaluation (CE) Explained:

- **Purpose**: CE continuously monitors clearance holders for security risks in real time, reducing the need for traditional periodic investigations.
- **Monitors**: Financial records, criminal activity, foreign travel, and other risk indicators.
- **Who is Enrolled**: All clearance holders at TS/SCI and, increasingly, Secret levels.

CE's Impact on Periodic Reinvestigations:

- **Less Frequent PIs**: CE reduces the need for frequent PIs by addressing concerns as they arise.

- **Still Required for TS/SCI**: An SF-86 and formal review are still required every **6 years** for TS/SCI clearances, even with CE in place.

- **Secret Clearances**: Generally, retain the 10-year cycle but may benefit from fewer traditional PIs due to CE.

Key Points

- **SF-86** is required at regular intervals despite CE, primarily every 6 years for TS/SCI.

- **CE** supplements the reinvestigation process by monitoring continuously, potentially reducing traditional investigation frequency.

- **Break in Service** longer than 2 years generally requires a new SF-86 for clearance reinstatement.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Guide to National Security Clearances vs. Public Trust Positions

This guide provides a clear breakdown of the distinctions between **National Security Clearances** and **Public Trust Positions**, along with practical tips and essential details for individuals navigating federal roles.

Overview

Aspect	National Security Clearances	Public Trust Positions
Purpose	Access to classified information vital to national security	Suitability for sensitive but unclassified roles
Access	Confidential, Secret, or Top-Secret information	Sensitive government systems and data
Investigation Focus	National security risk assessment	Job suitability and trustworthiness
Levels	Confidential, Secret, Top Secret	Low, Moderate, High Risk
Reinvestigation	Periodic reinvestigation required	Periodic updates at agency discretion

1. National Security Clearances

Purpose: Enables access to classified information based on national security needs.

Levels and Impacts

- **Confidential**: Unauthorized disclosure could cause damage to national security.
- **Secret**: Unauthorized disclosure could cause serious damage to national security.
- **Top Secret (TS)**: Unauthorized disclosure could cause exceptionally grave damage to national security.

Investigation Types

- **Confidential & Secret**:
  - ✓ **Tier 3 Investigation**: Includes National Agency Checks, local agency checks, and credit checks.
- **Top Secret**:
  - ✓ **Tier 5 Investigation**: Formerly known as Single Scope Background Investigation (SSBI), involving a detailed review of personal, professional, and financial history, plus interviews with associates.

Reinvestigation Requirements

- **Confidential**: Every 15 years
- **Secret**: Every 10 years
- **Top Secret**: Every 5 years

Continuous Evaluation

Many agencies now implement **Continuous Evaluation (CE)** programs for ongoing automated monitoring of clearance holders, including credit checks and criminal activity monitoring.

2. Public Trust Positions

Purpose: Evaluates suitability for roles involving sensitive but unclassified data and critical systems.

Risk Levels

- **Low Risk**: Minimal sensitivity; involves basic background checks.
- **Moderate Risk (MBI)**: Positions with access to sensitive systems or data; moderate background investigations required.
- **High Risk (BI)**: Positions with significant responsibilities or access to critical systems; requires more comprehensive background checks.

Investigation Types

- **Moderate Risk (Tier 2)**:
    - ✓ Includes employment history, credit checks, education verification, and references.
- **High Risk (Tier 4)**:
    - ✓ Involves a full Background Investigation (BI), like a clearance investigation but less rigorous than Tier 5.

Reinvestigation Requirements

- Generally conducted only when issues arise or at the agency's discretion.

3. Key Differences

Aspect	National Security Clearance	Public Trust Position
Governing Body	DoD or federal security agencies	Office of Personnel Management (OPM)
Investigation Depth	Rigorous, national security focus	Moderate to high, suitability focus
Eligibility	U.S. citizenship required	Often requires U.S. citizenship or permanent residency
Focus	National security risks	Job-related trustworthiness

4. Eligibility Criteria

National Security Clearances

- **U.S. Citizenship**: Required.
- **Vetting Areas**:
    - ➤ Criminal background
    - ➤ Financial stability
    - ➤ Foreign contacts/influence
    - ➤ Substance use history

Public Trust Positions

- **U.S. Citizenship or Residency**: Often required.
- **Suitability Focus**:

- ➢ Financial stability
- ➢ Employment history
- ➢ Character and trustworthiness

5. Reciprocity
- **Clearance Portability**: National Security Clearances can often transfer between agencies, but the process may involve verification delays.
- **Public Trust Portability**: Typically, not portable; suitability is reassessed by each agency.

6. Time to Obtain

Designation	Typical Processing Time
Confidential/Secret Clearance	1–6 months (may vary)
Top Secret Clearance	6 months to over a year (expedited for critical roles)
Low Risk Public Trust	Few weeks
Moderate Risk Public Trust	1–3 months
High Risk Public Trust	3–6 months

7. Frequently Asked Questions (FAQ)
1. **Can I hold both a clearance and a Public Trust designation?**
   Yes, many individuals hold both simultaneously.
2. **What happens if my clearance or designation is denied?**
   You'll receive a formal denial notice and often have the option to appeal through a designated process.
3. **Does my clearance or designation expire?**
   Clearances require periodic reinvestigations. Public Trust designations generally remain valid unless reviewed by the agency.

8. Common Myth
"Public Trust is a clearance."
False. Public Trust is a designation assessing job suitability, not national security access.

9. Final Tips
- **Higher Clearance Levels**: A Top Secret (TS) clearance often exceeds Public Trust requirements but confirm with the agency.
- **Maintain Documentation**: Keep forms like SF-86 updated to streamline future reviews.
- **Be Proactive**: Communicate with security officers and hiring managers to ensure smooth transitions.

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Breaking into Government Contracting Without Experience:

If you're new to government contracting, you might think the lack of experience, or a security clearance is a roadblock. The truth? It's challenging but **doable**—and with the right strategy, you can position yourself for success. Here's how to break in, stand out, and set yourself up for long-term growth.

Step 1: Understand the Industry

The government contracting world is vast and includes work in everything from IT and engineering to logistics and program management. Here's what you need to know:

- **Prime Contractors**: These companies work directly with the government.

- **Subcontractors**: These firms partner with primes to fulfill contract requirements

- **Security Clearance is Critical**:

  - A clearance is often required for roles, and many jobs specify the **type of clearance** (e.g., Secret, Top Secret, TS/SCI, TS/SCI/FSP).

  - **Most companies will NOT sponsor a clearance upfront**. If you don't have one, start with roles that don't require a clearance and work your way up.

  - **Pro Tip**: Take a role with a company that doesn't require a clearance or only needs a lower-level clearance. Show loyalty and deliver results. After some time, request to work on projects that require a higher-level clearance—companies are more likely to sponsor you once you've proven yourself.

Step 2: Identify Transferable Skills

Even without direct experience in the field, your existing skills can make you a strong candidate. Examples include:

- ✓ **Project Management**: Leading initiatives, managing deadlines, and delivering outcomes.

- ✓ **Administrative Skills**: Document management, scheduling, and maintaining compliance records.

- ✓ **Technical Expertise**: IT support, network troubleshooting, or cybersecurity knowledge.

- ✓ **Military or Public Sector Experience**: Veterans or those with public sector experience often have directly transferable skills.

Pro Tip: Speak the language of the industry. Use terms like "program support," "compliance monitoring," or "contract deliverables" when describing your experience, even if it's from another field.

Step 3: Tailor Your Resume

Your resume needs to meet the expectations of this highly competitive field. Here's how to stand out:

- ✓ **Highlight Transferable Skills**: Link your experience to contract-specific needs like project support, data analysis, or technical documentation.

- ✓ **Include Keywords**: Use terminology found in job descriptions (e.g., "Federal Acquisition Regulations," "classified environments").

- ✓ **List Clearances or Clearance Eligibility**: If you already hold a clearance or are eligible, mention it prominently.

- ✓ **Quantify Achievements**: Showcase results (e.g., "Coordinated efforts that reduced processing time by 25%").

Step 4: Build Industry-Specific Expertise

If you lack experience, **certifications** are a fast way to demonstrate your interest and commitment.

- **Highly Valued Certifications**:
  - ➢ **Project Management**: PMP, CAPM
  - ➢ **Cybersecurity**: CompTIA Security+, CISSP
  - ➢ **IT & Networking**: ITIL, AWS certifications
  - ➢ **Acquisitions/Contracting**: DAU Certifications (Defense Acquisition University)

Pro Tip: Pair certifications with networking—highlight your progress in LinkedIn posts or communities.

Step 5: Focus on Entry Points

Not all roles in the industry require experience or a clearance. Look for positions such as:

- ✓ **Administrative Assistant or Program Coordinator**: Support contract teams with scheduling, documentation, and logistics.
- ✓ **Analyst Roles**: Start as a junior data, financial, or operations analyst.
- ✓ **IT Support or Help Desk**: Technical support roles are often entry-level and don't require clearances.

Pro Tip: Some companies with large contracts (like Leidos or Peraton) hire for entry-level roles where they may sponsor a clearance after you've demonstrated your capabilities.

Step 6: Build Relationships

Networking is essential for breaking into this field.

- ✓ **LinkedIn**: Join groups like Cleared & Confused or job boards. Engage with posts, share insights, and connect with recruiters.
- ✓ **Recruiting Firms**: Use agencies that specialize in placing candidates in government contract roles (e.g., Tier One Talent & Intel Recruiting).
- ✓ **Job Fairs**: Attend virtual and in-person events to meet recruiters and learn about companies hiring entry-level talent.

Pro Tip: Reach out directly to recruiters and hiring managers—many roles are filled through referrals or direct applications.

Step 7: Prioritize Companies That Sponsor Clearances

While most companies don't sponsor clearances initially, some are known for clearance sponsorship:

- **CACI, Leidos, ManTech**: Known to sponsor clearances for roles where it's required.
- **Subcontractors**: Subcontracting firms often hire entry-level candidates and invest in their long-term growth.

Pro Tip: When interviewing, ask about clearance sponsorship opportunities and career advancement plans.

Step 8: Stay Persistent and Flexible

Breaking into this industry can take time, so don't get discouraged. Use each application as an opportunity to refine your approach.

Pro Tip: Take short-term contract roles to get your foot in the door—these can lead to long-term positions once you prove your value.

<div align="center">

Tier One Talent: Here to Help You Succeed

</div>

At **Tier One Talent**, we're dedicated to helping you navigate your career in government contracting. Here's how we support you:

- ✓ **Open Roles**: We post new opportunities weekly on the **Cleared & Confused** LinkedIn group.

- ✓ **Free Resume Reviews and Revisions**: We'll help you tailor your resume to the industry at no cost.

- ✓ **Always Available**: Got questions or need guidance? Reach out—we're happy to help!

Other available guides are free to download – All can be found on Cleared & Confused or Tier1-Talent.com under the job seeker tab!

- ✓ Contracting Pay & Schedule Essentials – A Candidate's Guide
- ✓ Government Contracts and Job Stability
- ✓ Security Clearance Comprehensive Overview
- ✓ Understanding Salary Rates on Government Contracts
- ✓ Government Contracting Guide 2024
- ✓ The Ultimate Cleared Professional Resource Guide 2024
- ✓ Cleared & Confident – The GovCon Professional's Guide to Salary Negotiation
- ✓ The No BS Resume Guide 2025 Edition
- ✓ The Ultimate GovCon Survival Guide 2024 – All Guides Combined
- ✓ Pro Tips Guide – Navigating the World of Recruiters like a Pro
- ✓ Guide to National Security Clearances vs. Public Trust Positions

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Government Contracts and Job Stability: A Quick Guide for Candidates

Navigating a career through government contracting can be unique and different from traditional corporate jobs. Here's a quick breakdown of how government contracts work and what to expect in terms of job stability and opportunities.

---

1. Understanding Government Contracts:

- **Purpose**: Government agencies outsource specific tasks to private companies, known as contractors, to support missions ranging from national defense to public administration.

- **Types of Contracts**:

  - ✓ **Fixed-term contracts**: Defined timeline with a set budget and deliverables (e.g., 1-5 years).

  - ✓ **Indefinite Delivery/Indefinite Quantity (IDIQ)**: Allows flexibility with time and quantities, often used for ongoing support.

- **Contractors Involved**:

  - ✓ **Prime Contractor**: Holds the main contract with the government.

  - ✓ **Subcontractors**: Support the prime contractor by supplying specific skills or roles.

---

2. Contract Phases and Employee Implications:

- **Award Phase**: Contracts are awarded after a competitive bidding process. When a company wins, roles need to be filled quickly.

- **Performance Phase**: During this time, the contractor fulfills the terms of the contract by hiring and assigning staff.

- **Renewal/Transition**: Toward the end of a contract, companies may pursue contract renewal. If the contract is awarded to a different company, they may absorb existing employees.

Job Stability Tip: Contracts often run for several years, but there can be a re-bid process at the end. Employees may transition to a new employer if the contract shifts hands, preserving continuity in roles.

---

3. Common Myths About Job Stability:

- **Myth**: "Contracts can end at any time."

  - o **Reality**: While government funding can fluctuate, contracts have built-in terms and aren't typically cut short without cause. Contractors aim to complete the contract period to secure renewal opportunities.

- **Myth**: "You'll lose your job if the contract changes hands."

  - o **Reality**: Employees are often retained by the new contractor because of their expertise and familiarity with the project.

---

4. Benefits of Working on a Government Contract:

- **Specialized Work**: Many roles are mission-critical, providing stable work in specialized fields like cybersecurity, data analysis, and intelligence.

- **Networking and Experience**: Contracts can expose employees to diverse federal agencies, fostering valuable connections and industry insight.

- **Skill Development**: Many positions on government contracts provide training and certifications to meet federal standards, adding to long-term career value.

---

5. Transitioning Between Contracts:

- **Job Continuity**: When a contract ends or transitions, employees can often stay in their roles under the new contractor.

- **Clearance Retention**: Security clearances transfer between contracts and employers, making candidates with clearances highly valuable.

Quick Tips for Candidates

- **Ask About Contract Length and Renewal**: Find out the duration of the contract and renewal options, which can give insight into stability.

- **Keep Updated on Agency Needs**: Agencies with continuous or expanding missions (like Defense or Intelligence) often provide steady contract work.

- **Stay Connected**: If a contract changes hands, networking with key stakeholders can improve the likelihood of staying on the project.

In summary, government contracts offer both stability and opportunities for professional growth. Understanding the process helps you navigate roles more confidently and plan for a sustainable career in the field.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Government Contracting Pay & Schedule Guide: Understanding Non-Exempt Roles

In government contracting, pay structures can be complex, especially for salary non-exempt roles. These positions are paid hourly but marketed as salary positions, which means you're compensated for all hours worked but typically without an overtime (OT) premium. Here's a guide to break down the essentials, including CONUS (domestic) and OCONUS (overseas) rates, standard work schedules, and different shift types.

1. Salary Non-Exempt: What It Means:

- Hourly Pay with "Salary" Label: In a salary non-exempt role, you're given an hourly rate but marketed as a salaried employee. You're paid for all hours worked, often with variations in hours based on specific contract requirements, but there's no time-and-a-half or double-time for extra hours.

- Paid for All Hours Worked: You're compensated for each hour you work, whether that's 84 hours in a two-week period or more, depending on the shift schedule.

2. Pay Differences Between CONUS and OCONUS:

- CONUS (Continental U.S.): Standard domestic rates apply, with hourly pay set according to U.S.-based cost of living and government labor standards.

- OCONUS (Outside Continental U.S.): Rates are often higher due to overseas allowances, cost of living adjustments, or hazard pay, depending on the location. OCONUS roles in high-risk areas may include added incentives for working in challenging environments.

Example:

- CONUS Rate: $50/hour → Paid for every hour worked at this rate.

- OCONUS Rate: $65/hour → Higher rate reflects added location-based incentives.

3. Standard Pay Schedule: 84-Hour vs. 80-Hour Workweeks:

- 84-Hour Pay Schedule: Many government contracts follow an 84-hour biweekly schedule instead of the traditional 80 hours. This often applies to shift-based roles, like those requiring a rotating or extended schedule.

Example:

- ✓ 84-Hour Schedule: 7 days on, 7 days off. In a two-week period, you'd work 84 hours, paid at your standard hourly rate.

- ✓ 80-Hour Schedule: A typical 40-hour workweek for two weeks, totaling 80 hours.

4. Common Shift Schedules and Their Impact on Pay:

Government contracts often require shift-based work to provide continuous coverage. Here are a few common shift types:

- Panama Schedule: A 2-2-3 rotation (2 days on, 2 days off, 3 days on) totaling 84 hours over two weeks.
  - ✓ Example: If paid $50/hour, biweekly pay would be $50 x 84 = $4,200.

- Swing Shift: Later hours, often from late afternoon to midnight. This shift may have a premium if the contract includes a shift differential.

- 12-Hour Rotating Shift: Employees work 12-hour shifts in rotations, such as 4 days on, 4 days off. Over two weeks, this might add up to 84 hours.

Example for a 12-Hour Shift Schedule:

- Hourly Rate: $60

- Biweekly Pay: $60 x 84 = $5,040

- 24/7 Coverage Schedules: Some contracts require continuous 24/7 coverage with rotating shifts (morning, swing, night), usually in an 84-hour biweekly cycle.

5. Shift Differentials, Weekend, and Holiday Pay

Some contracts offer additional pay, known as shift differentials, to employees scheduled on nights, weekends, or holidays.

1. Night Shift Differential: Extra pay for night shifts. Commonly 5-10% above base pay.
   - ✓ Example: Base Rate: $50/hour, Night Shift: $55/hour.
2. Weekend Pay: Some contracts offer a premium for weekend shifts (Saturday and Sunday).
   - ✓ Example: Base Rate: $50/hour, Weekend Differential: $3/hour, Total: $53/hour for weekend shifts.
3. Holiday Pay: Higher pay rate for shifts worked on holidays. Commonly 15-20% above base rate.
   - ✓ Example: Base Rate: $50/hour, Holiday Differential: $10/hour, Total: $60/hour on holidays.

Combined Differential Example:

- Scenario: You work a holiday weekend night shift.
- Saturday Night (Weekend + Night Shift): Base $50 + Night $5 + Weekend $3 = $58/hour
- Sunday Night (Holiday + Night Shift): Base $50 + Night $5 + Holiday $10 = $65/hour

6. Target Margins and Pay Structures Across Contracts

Margins vary by contract type, affecting final pay rates:

1. Cost-Plus Contracts: Lower margins (typically 8%-15%), as government reimburses costs plus a set fee.
2. Fixed-Price Contracts: Higher margins (15%-25%) due to the contractor assuming cost-overrun risks.
3. Labor-Intensive Subcontracts: Higher margins (20%-30%) in competitive fields like tech or cybersecurity to attract and retain skilled talent.

Key Takeaways for Candidates

- Check Pay Details: Verify your schedule, hourly rate, and any applicable shift differentials with your recruiter.
- Understand Required Shifts: If your schedule includes weekends or holidays, you'll likely be expected to work those shifts if they fall within your scheduled work period.
- Ask About Differentials: Not all contracts offer night, weekend, or holiday differentials, so clarify if these apply.

Disclaimer: This guide provides an overview of common pay structures and schedules in government contracting, but every contract, company, and program may differ. It's best to confirm specific details with your employer or recruiter to understand your exact pay structure.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Cleared & Confident: The GovCon Professional's Guide to Salary Negotiation

Introduction: The Importance of Knowing Your Worth

Knowing your worth is the cornerstone of navigating salary negotiations, especially in the highly competitive GovCon sector. Undervaluing yourself can lead to missed opportunities for fair compensation, while overvaluing can price you out of consideration. Striking the right balance is key confidence without overzealousness, realism without underselling your value.

This guide serves as a baseline to help you understand your market value and prepare for effective negotiations in the GovCon world and beyond. The more informed you are, the better equipped you'll be to advocate for what you deserve.

Understanding Your Market Value

1. **Leverage Salary Surveys:**

   ✓ [Government Contractors Compensation Survey](#): Offers detailed data for over 700 roles in GovCon companies.

   ✓ [Deltek Clarity Study](#): Provides insights on financial performance, labor trends, and compliance in the GovCon industry.

2. **Explore Tailored Compensation Tools:**

   ✓ [ClearanceJobs Calculator](#): Reveals salary trends based on role, location, and clearance level. Average salaries for cleared professionals in 2024 hit $114,946, with premiums for higher clearances and polygraphs.

3. **Review Job Postings for Salary Information:**

   ✓ Check for Listed Salaries: Look for salary ranges on job postings to understand typical compensation for similar roles.

   ✓ Compare Across Similar Roles: Assess multiple listings to identify the average pay for your qualifications and experience.

4. **Evaluate the Total Compensation Package:**

   ✓ Don't Stop at Base Salary: Weigh in benefits like health insurance, retirement plans, paid time off, and training opportunities. These can significantly enhance the overall value of the offer.

   ✓ Bonuses and Incentives: Check for signing bonuses, performance bonuses, or additional financial perks.

   ✓ Professional Development: Consider opportunities for certifications, training, and career advancement.

5. **Ask Around:**
   Speak with peers, recruiters, and mentors who know the industry. Their insights can help you understand salary benchmarks, company reputation, and negotiation strategies.

6. **Gather All Information Before Proceeding with an Offer:**
   Ensure you have a clear understanding of base salary, benefits, job responsibilities, and growth opportunities. Comprehensive research positions you to make informed decisions.

Special Note: The more informed you are, the better equipped you'll be to negotiate a salary that reflects your worth considering the bigger picture of total compensation.

Preparing for Negotiation

1. Understand the Role and Its Requirements

✓ Position Type: Differentiate between W-2 (employee), 1099 (independent contractor), and subcontractor roles, as each comes with unique compensation structures and benefits.

✓ Exempt vs. Non-Exempt: Determine whether the role is eligible for overtime pay.

2. Shop Around, but Avoid Common Pitfalls

It is recommended to shop around and find the best total offer that works for you and your family. However, exercise caution when accepting offers or Conditional Offer Letters (COLs) with one company while continuing to entertain offers from others, especially for the same contract.

GovCon is a small, tightly connected industry, and your actions can have long-term repercussions. Engaging in practices like "contract hopping" or reneging on signed agreements can harm your reputation and may result in being blacklisted from specific contracts or even entire programs.

Example of Negative Impact:

Consider this scenario:

- ✓ You accept a COL with Company A: Company A submits your profile for approval on a high-profile contract.

- ✓ You continue entertaining offers with Company B: After Company A's submission, you accept an offer from Company B for the same contract but at a slightly higher pay rate. Company B submits your profile as well.

- ✓ The outcome: The customer notices your dual submissions and removes you from consideration entirely. Both companies are informed, and your actions reflect poorly on your integrity. This not only damages your reputation with the companies involved but also with the program manager overseeing the contract, who may spread the word to others in the GovCon network.

Special Note: Many companies enforce non-compete agreements or policies that prohibit candidates from pursuing multiple offers for the same contract. Violating these agreements can result in disqualification, legal implications, or permanent damage to your professional relationships.

During the Negotiation

1. Communicate Your Value

- ✓ **Express Enthusiasm:** Show genuine interest in the role and organization. Employers value candidates who are excited about the position and its potential impact.

- ✓ **Present Data-Driven Arguments:** Reference market rates, industry benchmarks, and your unique qualifications during discussions. Use clear, factual evidence to support your desired salary.

2. Be Transparent and Ethical

- ✓ **Disclose Early:** If you are considering multiple offers, communicate this professionally to avoid conflicts or ethical concerns. Transparency demonstrates integrity and builds trust.

- ✓ **Maintain Industry Relationships:** The GovCon sector is a small, connected community. Acting ethically ensures you maintain a positive reputation with employers and peers.

3. Stay True to Yourself

- ✓ **Be Authentic:** Don't feel pressured to oversell or undersell yourself. Highlight your skills, experiences, and accomplishments honestly, as they are the foundation of your value.

- ✓ **Avoid Overextension:** If the position is the right fit, the negotiation and interview process will flow naturally. You won't need to overpromise or stretch beyond your genuine capabilities to secure the role.

- ✓ **Trust the Process:** Focus on roles that align with your background and goals. The right opportunity will complement your strengths, allowing you to confidently present your qualifications without compromising your authenticity.

Special Note: By staying true to yourself and approaching negotiations with honesty and enthusiasm, you'll create a foundation of trust and ensure that the position is a mutual fit for both you and the organization.

After the Negotiation

1. Show Gratitude and Follow Up

- ✓ **Thank the Hiring Team:** Express appreciation for the opportunity to interview or discuss the position. A simple "Thank you for taking the time to speak with me today" can leave a lasting positive impression.

- ✓ **Ask Questions:** If you have concerns or need clarification, don't hesitate to ask thoughtful questions about the role, team, or next steps.
- ✓ **Solicit Feedback:** Politely request feedback on your performance during the process. This shows humility and a willingness to improve, even if an offer isn't extended.
- ✓ **Write a Thank-You Email:** Send a professional thank-you email within 24 hours of your conversation. Reiterate your enthusiasm for the role and summarize key points discussed. Even if you don't receive an offer, this keeps doors open for future opportunities.

2. Obtain Written Confirmation

- ✓ **Document All Terms:** If an offer is made, ensure all agreed-upon terms—salary, benefits, and any special agreements—are clearly outlined in writing. If it's not in writing, it doesn't count.
- ✓ **Clarify Before Signing:** Take time to review the offer letter thoroughly and address any discrepancies or unclear terms.

3. Evaluate the Offer Holistically

- ✓ **Big Picture Analysis:** Consider how the role fits with your career goals, work-life balance, and long-term aspirations. Assess the benefits package, professional growth opportunities, and company culture as part of your decision-making process.

4. Avoid Over-Negotiation

- ✓ **Honor Your Commitment:** Once you accept an offer, commit to it.

Key Takeaways

- ✓ **Knowing your worth empowers you to negotiate effectively and fairly.**
- ✓ **Shop around for the best total offer but prioritize integrity to avoid damaging your reputation.**
- ✓ **Evaluate total compensation packages, not just base salary.**
- ✓ **Avoid actions that may lead to being blacklisted, such as entertaining multiple offers for the same contract or violating non-compete agreements.**
- ✓ **Always be prepared, professional, and realistic during negotiations.**

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Beginner's IT Career Roadmap for Cleared Individuals

Got a clearance? Great—if you're looking to break into the defense or GovCon IT world, you're already ahead. But having a clearance is just the beginning. Here's your practical, no-nonsense guide to turning it into a rewarding IT career. Let's get started

Step 1: Lay the Groundwork

Before you dive into the IT ocean, you need to learn how to swim. Start here:

- **CompTIA A+**: The ultimate beginner's cert. Covers hardware, software, troubleshooting, and even a bit of networking. Think of it as the Swiss Army knife of IT certs.
- **Google IT Support Professional Certificate**: Learn troubleshooting, networking basics, and customer service skills. Bonus: It's free with a Coursera trial.
- **Microsoft Azure Fundamentals**: Because cloud computing isn't going anywhere. Azure is a major player, and this cert gets you in the game.

Goal: Understand the basics so you can confidently nod along in meetings and troubleshoot without calling for backup.

Step 2: Grab Your Starter Certifications

Certs are your IT passport. These entry-level ones will get your foot in the door:

- **CompTIA Security+**: A must for cleared IT jobs. It covers basic cybersecurity concepts and is DoD 8570 compliant.
- **CompTIA Network+**: Teaches you how to configure, manage, and troubleshoot networks. Ideal if you're eyeing networking roles.
- **Cisco Certified Networking Associate (CCNA)**: Networking 101 with a Cisco twist. A solid choice for aspiring network admins.

Pro Tip: Don't just aim to pass—learn the material. The real world doesn't have cheat sheets.

Step 3: Land Your First IT Gig

You've got the skills & clearance; now it's time to get paid. Here's how:

- **Job Titles to Search:** IT Support Specialist, Help Desk Technician, Junior Network Admin, Entry-Level Cybersecurity Analyst.
- **Where to Look:** ClearanceJobs.com, LinkedIn, and major contractors like Lockheed Martin and Booz Allen Hamilton.
- **Resume Tip:** Put your clearance front and center. It's your VIP pass—don't bury it under "Hobbies: Loves long walks on the beach."

Goal: Get your first IT paycheck and start building that real-world experience.

Step 4: Keep Leveling Up

Once you're in the game, it's time to sharpen those skills. Check out these free training programs:

- **IBM Cybersecurity Fundamentals** (Coursera): A solid intro to cybersecurity concepts and trends.
- **AWS Cloud Practitioner Essentials** (AWS): Learn the basics of Amazon's cloud platform—a must-know for cleared IT pros.
- **Kubernetes Basics** (CNCF): Containers are everywhere. Learn the basics and start talking like a DevOps guru.

Goal: Add new tools to your IT toolbox so you're always one step ahead.

Step 5: Flex That Clearance

Your clearance is pure gold. Here's how to leverage it:

- **Highlight It Everywhere:** Your resume, LinkedIn, and every conversation with a recruiter.
- **Target Cleared Employers:** Think defense contractors, government agencies, and IT firms with federal contracts.
- **Mention It Early and Often:** Recruiters love candidates with clearances. Make sure they know you're ready to roll.

Goal: Use your clearance to land roles that others can't touch!

Step 6: Build Your Network

IT is a team sport, and networking is your playbook. Here's how to do it:

- **Cleared Job Fairs:** A goldmine for meeting recruiters and hiring managers.
- **LinkedIn Groups:** Join forums for cleared IT professionals and government contractors.
- **Find a Mentor:** Everyone in IT has that one person who showed them the ropes. Find yours.

Pro Tip: Ask questions, be curious, and don't be afraid to say, "I don't know." People love helping those eager to learn.

Step 7: Think Long-Term

You're in. Now it's time to plan your IT domination. Here's what's next:

Intermediate Certifications:

- **AWS Solutions Architect - Associate**: Take your cloud skills to the next level.
- **Certified Ethical Hacker (CEH)**: Perfect for aspiring cybersecurity pros.
- **CompTIA Linux+**: Learn the OS that powers everything from servers to supercomputers.

Advanced Certifications:

- **Certified Information Systems Security Professional (CISSP)**: The gold standard for senior cybersecurity roles.
- **Microsoft Certified: Azure Solutions Architect Expert**: Show off your advanced cloud skills.
- **Google Cloud Professional Architect**: Prove you can design complex cloud solutions.

Big Roles to Target: Cybersecurity Engineer, Cloud Architect, Systems Engineer.

Goal: Become the go-to expert in your niche and watch your career (and paycheck) soar.

Final Thoughts

Having a clearance is like getting a head start in a race—it gives you an edge. Pair that advantage with the right certifications, skills, and determination, and nothing can hold you back. Stay curious, keep building your knowledge, and remember success in IT is as much about connecting with people as it is about mastering technology. Best of luck—and welcome to the IT community!

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Quick Reference Guide: DoD IAM Certification Levels

IAM Levels Overview

The DoD 8570.01-M framework establishes **Information Assurance Management (IAM)** levels to define certification requirements for cybersecurity professionals managing systems and personnel. IAM certifications are divided into three levels: **I, II, and III**, with Level III being the highest tier.

IAM Level I (Entry-Level Management of Information Assurance Systems)

Focus: Basic system authorization and leadership tasks.

Certifications:

1. **CAP** – Certified Authorization Professional
2. **GSLC** – GIAC Security Leadership Certification
3. **Security+ CE** – CompTIA Security+ (Continuing Education version)

IAM Level II (Intermediate-Level Management of Information Assurance Systems)

Focus: Intermediate management, risk assessment, and compliance tasks.

Certifications:

1. **CAP** – Certified Authorization Professional
2. **CASP+ CE** – CompTIA Advanced Security Practitioner (Continuing Education version)
3. **CISM** – Certified Information Security Manager
4. **CISSP (Associate)** – Certified Information Systems Security Professional (Associate level)
5. **GSLC** – GIAC Security Leadership Certification

IAM Level III (Advanced-Level Management of Information Assurance Systems)

Focus: Strategic and advanced system management, high-level risk mitigation, and leadership.

Certifications:

1. **CISM** – Certified Information Security Manager
2. **CISSP** – Certified Information Systems Security Professional
3. **GSLC** – GIAC Security Leadership Certification
4. **CCISO** – Certified Chief Information Security Officer

Beyond IAM Level III

Although **IAM Level III** is the highest formal tier in the framework, professionals can advance into senior and strategic roles by pursuing additional certifications and leadership opportunities.

Advanced Leadership Roles:

- **Chief Information Security Officer (CISO)**
- **Chief Risk Officer (CRO)**

Recommended Advanced Certifications:

1. **CISSP-ISSAP** – Information Systems Security Architecture Professional
2. **CISSP-ISSMP** – Information Systems Security Management Professional
3. **CCISO** – Certified Chief Information Security Officer
4. **CGEIT** – Certified in the Governance of Enterprise IT
5. **PMP** – Project Management Professional
6. **COBIT 5/COBIT 2019** – IT governance and management framework
7. **ITIL** – IT Service Management

DoD Cyber Workforce Framework (DCWF):

The new DCWF focuses on advanced roles in governance, operational execution, and enterprise-wide cybersecurity practices.

<div align="center">

Summary Table

</div>

IAM Level	Focus	Certifications
IAM Level I	Basic system authorization and leadership	CAP, GSLC, Security+ CE
IAM Level II	Intermediate risk management and compliance	CAP, CASP+ CE, CISM, CISSP (Associate), GSLC
IAM Level III	Strategic leadership and high-level risk mitigation	CISM, CISSP, GSLC, CCISO

Key Takeaways

- **IAM Level III** is the highest certification level in the DoD 8570.01-M framework.
- Advanced leadership roles and certifications go beyond Level III for professionals seeking broader strategic and executive opportunities.
- Senior roles often require additional certifications and specialized skills in governance, enterprise IT, and project management.

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Quick Reference Guide: DoD IAT Certification Levels

IAT Levels Overview

The DoD 8570.01-M framework establishes Information Assurance Technical (IAT) levels to define certification requirements for cybersecurity professionals performing technical and operational roles. IAT certifications are divided into three levels: I, II, and III, with Level III being the highest formal tier. Professionals can progress into senior and specialized roles beyond Level III by pursuing advanced certifications and leadership opportunities.

IAT Level I (Entry-Level Technical Roles)

Focus: Basic support and maintenance of IT systems, including hardware and software.

Certifications:

1. A+ CE – CompTIA A+ (Continuing Education version)
2. CCNA-Security – Cisco Certified Network Associate Security
3. CND – Certified Network Defender
4. Network+ CE – CompTIA Network+ (Continuing Education version)
5. SSCP – Systems Security Certified Practitioner

IAT Level II (Intermediate-Level Technical Roles)

Focus: Administration and support of IT systems with an emphasis on cybersecurity.

Certifications:

1. CCNA-Security – Cisco Certified Network Associate Security
2. CySA+ CE – CompTIA Cybersecurity Analyst (Continuing Education version)
3. GICSP – Global Industrial Cyber Security Professional
4. GSEC – GIAC Security Essentials Certification
5. Security+ CE – CompTIA Security+ (Continuing Education version)
6. SSCP – Systems Security Certified Practitioner

IAT Level III (Advanced-Level Technical Roles)

Focus: Advanced administration, security, and troubleshooting of IT systems.

Certifications:

1. CASP+ CE – CompTIA Advanced Security Practitioner (Continuing Education version)
2. CCNP-Security – Cisco Certified Network Professional Security
3. CISA – Certified Information Systems Auditor
4. CISSP – Certified Information Systems Security Professional
5. GCED – GIAC Certified Enterprise Defender
6. GCIH – GIAC Certified Incident Handler

Beyond IAT Level III

While IAT Level III is the highest formal tier in the framework, professionals can advance into senior and specialized roles by pursuing additional certifications and leadership opportunities.

Recommended Advanced Certifications Beyond IAT Level III:

1. **CISSP-ISSAP** – Information Systems Security Architecture Professional
2. **CISSP-ISSMP** – Information Systems Security Management Professional
3. **CCIE-Security** – Cisco Certified Internetwork Expert Security
4. **OSCP** – Offensive Security Certified Professional
5. **CCISO** – Certified Chief Information Security Officer
6. **CEHv12 Master** – Certified Ethical Hacker Master
7. **CGEIT** – Certified in the Governance of Enterprise IT
8. **GIAC Security Leadership Advanced Tracks**

Senior Roles Beyond IAT:

- **Chief Information Security Officer (CISO)** – Enterprise-wide security strategy and governance.
- **Chief Technology Officer (CTO)** – Technical leadership and innovation.
- **Senior Penetration Tester** – Offensive security and advanced vulnerability assessments.
- **Enterprise Architect** – Designing secure and scalable enterprise IT systems.
- **Cyber Operations Specialist** – Advanced offensive and defensive cyber operations.

Key Takeaways

- IAT Level III is the highest formal tier within the framework.
- Professionals can advance beyond Level III by acquiring specialized certifications and pursuing leadership roles.
- Advanced roles and certifications focus on enterprise IT governance, offensive and defensive cybersecurity, and technical leadership.

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/

Pro Tips Guide: Navigating the World of Recruiters Like a Pro

Recruiters can be powerful allies on your career journey—if you know how to work with them effectively. By understanding the different types of recruiters, their benefits, and red flags to watch for, you can confidently navigate the job market while protecting your interests.

How Recruiters Contact Candidates:

Recruiters use various methods to connect with job seekers, depending on their approach and the role they're hiring for. Here's what to expect:

1. **Cold Calls**
   - Some recruiters still use direct phone calls, especially in industries where immediate communication is key.
   - Be cautious with cold calls and verify the recruiter's identity.

2. **Online Communication**
   - LinkedIn messages, emails, or job board platforms (e.g., Indeed, Glassdoor) are the most common methods.
   - Always verify the sender's email address and LinkedIn profile for legitimacy.

3. **Sourced by a Recruiter**
   - If you've been "sourced," the recruiter likely found you through LinkedIn, a job board, or their internal database.
   - These opportunities are targeted to your background but verify that the role aligns with your goals.

4. **Contact After You Apply**
   - When you apply for a job through a company's website, you'll typically be contacted by an internal recruiter.
   - Internal recruiters work directly for the organization and often provide deeper insights into the role and company culture.

Benefits of Working with Recruiters:

Recruiters do more than just match candidates with jobs. Here are keyways they add value:

1. **Resume Optimization**
   - Recruiters often help polish your resume to align with specific roles, ensuring you stand out.

2. **Interview Preparation**
   - Recruiters provide guidance, including practice questions, tips, and insights about the hiring manager or company culture.

3. **Salary Negotiations**
   - Recruiters can advocate for you during salary and benefits discussions, leveraging their knowledge of industry benchmarks.
   - Pro Tip: Be clear about your expectations so the recruiter can negotiate effectively on your behalf.

4. **Bypassing the Applicant Tracking System (ATS)**
   - Third-party recruiters often have direct relationships with hiring managers, allowing your resume to skip the ATS and land directly on a decision-maker's desk.

5. **Access to Hidden Opportunities**

- Many roles, especially executive or specialized positions, aren't publicly advertised and are accessible only through recruiters.

6. **Support and Advocacy**
   - Recruiters can provide updates, follow up on your behalf, and ensure you're well-represented during the hiring process.

7. **Career Guidance**
   - Good recruiters stay updated on market trends, industry demands, and skill requirements, helping you make informed career decisions.

The Recruiter-Candidate Partnership:

Approach your relationship with recruiters as a partnership. Here's how to build a strong rapport:

1. **Be Transparent**
   - Share accurate information about your skills, goals, and availability. The more they know, the better they can represent you.

2. **Stay in Touch**
   - Even if a role doesn't work out, maintain contact with good recruiters. Connect on LinkedIn and share updates about certifications or career changes.

3. **Professional Communication**
   - Treat all interactions as part of the interview process. Timely, polite communication goes a long way in building trust.

4. **Respect Their Time**
   - Be responsive and follow through on agreed timelines. A recruiter's time is as valuable as yours.

A Warning About Signing a Right to Represent (R2R):

A Right to Represent (R2R) is a document some recruiters ask you to sign, granting them exclusive permission to submit your resume for a specific job. Here's what to know:

- **Not Always Necessary:** Signing an R2R is generally unnecessary unless working with a headhunter placing you in an executive-level role.

- **Read Before Signing:** Always review the document carefully to ensure it aligns with your interests. Research the recruiter, the role, and the hiring company before agreeing to exclusivity.

- **Red Flags in R2Rs**
   - Grant the recruiter broad, indefinite rights over your job search.
   - Prevent you from working with other recruiters or applying to other roles at the same company.
   - Lack specificity about the job or company.

Pro Tip: If a recruiter pressures you into signing an R2R without clear details, consider it a red flag.

Types of Recruiters: Understanding the types of recruiters helps set clear expectations.

1. **Internal Recruiters**
   - Work directly for the hiring company and focus on finding candidates aligned with its culture and goals.

2. **External Recruiters**

> - Work for agencies and represent multiple companies, focusing on filling roles efficiently.
3. **Technical Recruiters**
   - Specialized in hiring for IT, engineering, or other technical fields.
4. **Third-Party Recruiters**
   - Contracted by companies to assist internal teams in filling specific roles, often bypassing the ATS.
5. **Contingency Recruiters**
   - Paid only when they successfully place a candidate.
6. **Retained Recruiters**
   - Exclusively hired to fill high-level or specialized positions, often working on a retainer fee.
7. **Headhunters**
   - Target senior executives or highly specialized roles, often charging fees directly to the candidate.

RPO vs. Staffing Agencies:

Recruitment Process Outsourcing (RPO)

- Outsources an organization's entire recruitment function.
- Focuses on long-term talent acquisition, employer branding, and pipeline development.

Staffing Agencies

- Fill short-term, contract, or temporary roles.
- Tend to be more transactional, with less focus on long-term fit.

For Job Seekers:

- RPOs offer transparency and alignment with the company's goals.
- Staffing agencies can be hit-or-miss; some prioritize speed over quality.

Good vs. Bad Recruiter Checklist:

Good Recruiter	Bad Recruiter
Provides clear and transparent job details.	Vague about the role or employer.
Professional LinkedIn profile with a photo.	No picture or incomplete LinkedIn profile.
Communicates promptly and clearly.	Delayed or inconsistent communication.
Prepares you for interviews.	Pushes you into interviews unprepared.
Represents reputable clients.	Refuses to disclose company information.
Focused on your skills and career goals.	Treats you as just another number to fill a role.

Red Flags to Watch For: Stay vigilant for these warning signs:

1. **Requests for Personal Information Too Soon**
   - Never share your Social Security Number (SSN), banking info, or sensitive details early in the process.

2. **Pressure to Sign Exclusivity Agreements**
   - Be cautious about signing an R2R unless clear details are provided.
3. **Suspicious Contact Details**
   - Watch out for foreign numbers, generic email domains, or recruiters who can't verify their company.
4. **Unrealistic Job Offers**
   - If the salary or perks seem too good to be true, research the role thoroughly.
5. **Charging a Fee**
   - Recruiters are typically paid by employers, not candidates.
   - Exception: Headhunters may charge candidates directly, but this is rare and limited to high-level executive roles.

Pro Tips for Working with Recruiters

1. **Vet the Recruiter**
   - Check their LinkedIn profile, reviews, and professional background.
2. **Be Clear About Your Goals**
   - Communicate your career objectives, salary expectations, and desired roles early.
3. **Stay Professional**
   - Treat all interactions as part of the interview process.
4. **Protect Your Data**
   - Only share sensitive information after verifying both the recruiter and the job opportunity.
5. **Ask the Right Questions**
   - Who is the hiring company?
   - Why do you think I'm a good fit for this role?
   - What is the timeline for interviews and decisions?

Recruiters can open doors to incredible opportunities when you know how to engage with them strategically. By staying informed, proactive, and vigilant, you can build valuable partnerships while protecting yourself from potential pitfalls.

Remember, a great recruiter is your partner in success—not just someone filling a quota.

Have questions or concerns?

Tier One Talent & Intel Recruiting
Tier1-talent.com
sgagliardi@tier1-talent.com
910.850.3055
Cleared & Confused LinkedIn: https://www.linkedin.com/groups/13118066/