DOMINUS GRAY, LLC

Securing Access to Opportunity

Candidate Vetting & Qualification Process

Cybersecurity Talent Screening Methodology

February 10, 2026

Document ID: DG-CVP-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered

1. Process Overview

Dominus Gray employs a rigorous six-stage vetting pipeline to ensure every cybersecurity professional placed with our clients meets the highest standards of technical competence, security compliance, and cultural alignment. Our process is specifically designed for the defense and federal contracting ecosystem, where security clearance, mission readiness, and trustworthiness are non-negotiable.

Our vetting methodology yields a 95%+ retention rate at the 90-day mark, reflecting the thoroughness of our screening and the quality of our candidate-client matching approach.

Six-Stage Vetting Pipeline

1 **Stage 1: Sourcing & Initial Screen**
Resume review, availability confirmation, compensation alignment, initial phone screen

▼

2 **Stage 2: Technical Assessment**
Skills verification, certifications validation, hands-on technical interview

▼

3 **Stage 3: Security & Clearance Verification**
Active clearance verification via DCSA/DISS (JPAS fully decommissioned), CUI handling training verification, background check, 3 professional references

▼

4 **Stage 4: Cultural & Mission Fit**
Behavioral interview, client culture alignment, communication assessment

▼

5 **Stage 5: Client Presentation**
Candidate profile package, skills matrix, coordinated interview scheduling

▼

6 **Stage 6: Onboarding & Integration**
First-day preparation, 30/60/90-day check-ins, performance monitoring

2. Sourcing Channels

Dominus Gray leverages a diversified sourcing strategy to access the deepest pools of cleared cybersecurity talent. Our multi-channel approach ensures broad reach while maintaining quality and compliance with diversity objectives.

ClearanceJobs.com

PRIMARY

Primary platform for cleared professionals. Active presence with featured employer status for TS/SCI and Secret-cleared cybersecurity talent.

LinkedIn Recruiter

DIRECT

Direct sourcing through advanced search, InMail campaigns, and targeted outreach to passive candidates with verified cybersecurity backgrounds.

Diversity Cyber Council Network

DIVERSITY

Strategic partnership providing access to veteran and underserved community pipelines, supporting diversity hiring objectives for federal contracts.

Dominus Gray Alumni Network

PROPRIETARY

Dominus Gray's proprietary talent network of graduates from internal development programs, producing job-ready cybersecurity professionals with hands-on training and mentorship.

DoD SkillBridge Program

MILITARY

Transitioning service members completing their final 180 days of military service, offering unparalleled security awareness and mission focus.

CyberVetsUSA Program Participants

VETERAN

Veterans with cybersecurity training and certifications seeking civilian career opportunities in the defense industrial base.

Professional Referral Network

REFERRAL

Employee and contractor referral program incentivizing introductions to qualified cleared professionals from existing trusted contacts.

AFCEA / ISSA / ISACA Chapters

PROFESSIONAL

Active engagement with professional association chapters providing access to certified, career-committed cybersecurity practitioners.

3. Technical Assessment Criteria

Technical assessments are tailored to the specific role type and client requirements. Each candidate undergoes a structured evaluation covering core competencies, tool proficiency, and real-world scenario analysis.

• Security Analyst

COMPETENCY AREA	ASSESSMENT CRITERIA
SIEM Proficiency	Splunk, Sentinel, QRadar — query writing, dashboard creation,
Incident Triage	Alert prioritization, escalation procedures, playbook execution
Threat Intelligence	MITRE ATT&CK mapping, IOC analysis, threat hunting
Log Analysis	Windows/Linux event logs, network flow analysis, correlation

• Security Engineer

COMPETENCY AREA	ASSESSMENT CRITERIA
Network Security	Firewall management, IDS/IPS, network segmentation, zero-trust
Cloud Security	AWS/Azure/GCP security controls, IAM policies, cloud-native tools
Automation	Python/PowerShell scripting, SOAR platforms, CI/CD security
Infrastructure	Hardening, STIG implementation, vulnerability management

• Compliance Analyst

COMPETENCY AREA	ASSESSMENT CRITERIA
NIST Frameworks	NIST 800-171, 800-53, CSF — control assessment and gap
Audit Experience	Internal audits, C3PAO preparation, evidence collection, POA&M management
Documentation	SSP writing, policy development, procedure creation, CMMC
Regulatory Knowledge	DFARS 252.204-7012, ITAR, FedRAMP, FISMA compliance requirements

• Penetration Tester

COMPETENCY AREA	ASSESSMENT CRITERIA
Certifications	OSCP, CEH, GPEN, GWAPT — verified through issuing body
Methodology	OWASP, PTES, NIST SP 800-115 — structured testing approach
Tool Proficiency	Burp Suite, Metasploit, Nmap, BloodHound, Cobalt Strike
Reporting	Executive summaries, technical findings, risk ratings, remediation guidance

Certification Validation Process

All candidate certifications are verified directly through the issuing body (e.g., (ISC)², CompTIA, ISACA, Offensive Security). Dominus Gray maintains verification records and provides certification status documentation to clients as part of the Candidate Profile Package.

4. Security Clearance Verification

Dominus Gray operates within strict compliance protocols to verify active security clearances for all candidates placed in positions requiring access to classified or controlled information.

4.1 Verification Process

- Candidate self-reports clearance type, level, and investigation date during initial screen
- Dominus Gray's Facility Security Officer (FSO) initiates verification through DCSA/DISS (the current verification system, replacing the fully decommissioned JPAS)
- Cross-reference candidate-provided information with official records
- Verify clearance is active (not expired, suspended, or revoked)
- Confirm polygraph status where applicable (CI or Full Scope)
- Verify candidate CUI handling training completion and CMMC awareness
- Document verification results in candidate file with date stamp

4.2 Required Documentation

- Government-issued photo identification (two forms)
- SF-86 submission confirmation (candidate attestation)
- Clearance sponsorship transfer documentation (if changing sponsors)
- Continuous Evaluation (CE) enrollment confirmation
- Any interim clearance documentation (if applicable)

4.3 DCSA/DISS Verification Steps

1. FSO logs into DISS (Defense Information System for Security)
2. Initiates Subject Ownership query for the candidate
3. Reviews investigation type, scope, and adjudication date
4. Confirms clearance level and access eligibility
5. Documents verification with screenshot/record for audit trail

6. If transfer required, initiates in-scope transfer request
7. Monitors transfer status and confirms completion before start date

Clearance Compliance Notice

Dominus Gray does not access or store classified information during the verification process. All clearance verifications are conducted through authorized government systems by credentialed personnel. Candidates are never asked to provide classified details about their investigations or assignments.

5. Quality Metrics & Performance Standards

Dominus Gray tracks key performance indicators across the entire vetting pipeline to ensure consistent quality, continuous improvement, and client satisfaction.

TIME TO FILL	4-8 wks	Target fill timeline
CANDIDATE:INTERVIEW	3:1	Submission to interview ratio
INTERVIEW:PLACEMENT	2:1	Interview to placement ratio
90-DAY RETENTION	95%+	Target retention rate
CLIENT SATISFACTION	4.5/5	Target satisfaction score
CUI TRAINING RATE	100%	Before first day of placement

Continuous Improvement Tracking

- Monthly pipeline analytics reviewed by recruiting leadership
- Quarterly client satisfaction surveys with actionable feedback loops
- Annual process audit with documented improvements and corrective actions
- Real-time dashboard tracking of all pipeline stage conversion rates
- Post-placement debrief with client and candidate at 30, 60, and 90 days

6. Candidate Profile Package

When presenting candidates to clients, Dominus Gray provides a comprehensive Candidate Profile Package designed to give hiring managers complete visibility into each candidate's qualifications, experience, and fit for the role.

Package Contents

Sanitized Resume

Professionally formatted resume with candidate's personal identifying information protected until client expresses interest. Highlights relevant experience, certifications, and technical skills aligned to the specific role.

Skills Matrix

Detailed competency mapping against the SOW requirements, showing proficiency levels (Expert / Proficient / Familiar) for each required and preferred skill.

Technical Assessment Scores

Results of Dominus Gray's internal technical assessment, including scenario-based evaluation scores and interviewer notes.

Reference Summary

Consolidated summary of three (3) professional reference checks, including relevance to the role, performance feedback, and overall recommendation strength.

Clearance Status

Verified clearance level, type of investigation, investigation date, and current status (Active / Interim / In Process). Polygraph status noted where applicable.

Availability & Start Date

Confirmed earliest available start date, notice period requirements, and any scheduling constraints.

Rate Information

Proposed bill rate aligned to the SOW budget, with any rate variations noted for overtime, travel, or shift differential.

Candidate Privacy & Compliance

All candidate information is handled in compliance with applicable privacy laws and regulations. Personal identifying information is only shared with the client upon mutual agreement to proceed to the interview stage. Dominus Gray maintains candidate data in accordance with its Privacy Policy and applicable federal/state data protection requirements.

7. About Dominus Gray

Dominus Gray, LLC is a Service-Disabled Veteran-Owned Small Business (SDVOSB) headquartered in Houston, Texas. We specialize in cybersecurity staffing, workforce development, and compliance consulting for the defense industrial base and federal contracting community.

Our Differentiators

- SDVOSB certified — eligible for veteran set-aside contracts
- Deep expertise in cleared cybersecurity talent placement
- Proprietary Career Acceleration Program producing job-ready professionals
- Strategic partnerships with military transition programs (SkillBridge, CyberVetsUSA)
- Rigorous six-stage vetting pipeline with 95%+ retention rate
- Dedicated account management and 30/60/90-day placement support
- CMMC-aware staffing — understanding of CUI handling and compliance requirements

Contact Information

Company:	Dominus Gray, LLC
Address:	5866 East Post Oak Lane, Houston, Texas 77055
Phone:	(346) 542-0471
Email:	odie.gray@dominusgray.com
Website:	www.dominusgray.com
Cage Code:	Registered on SAM.gov
Certifications:	SDVOSB | MBE | NaBOVA | VetHUB