CAPABILITY STATEMENT

Microsoft 365 Governance, Identity, Threat Protection, Network Security, Virtualization, Records Management, and Compliance Translation for Federal and Regulated Commercial Environments.

QUICK FACTS

Legal Name	Soulier Group LLC
Unique Entity ID (UEI)	**HUJFDP334G53**
CAGE Code	**1ZZP6** (assigned 2026-05-07)
Entity Type	Wisconsin LLC (single-member, disregarded entity)
Primary NAICS	541512: Computer Systems Design Services
Additional NAICS	541519, 541611, 541690, 518210, 541513, 561621
Size Standard	Small Business at all NAICS sizes
State of Formation	Wisconsin (organized 2026)
Principal Place of Business	Wisconsin

Socioeconomic Certifications

✓ **Indian Economic Enterprise (IEE), Buy Indian Act** (FAR 52.212-3 self certified)

✓ **Small Disadvantaged Business (SDB):** FAR 52.212-3 self certified (Native American social-disadvantage presumption per 13 CFR 124.103; economically disadvantaged per 13 CFR 124.104)

✓ **Native American Owned** (enrolled member, Lac du Flambeau Band of Lake Superior Chippewa Indians of the Lac du Flambeau Reservation of Wisconsin)

✓ **Minority Owned Business**

◤ **SBA 8(a) Business Development Program:** application targeted for September 2026 submission

CAPABILITY DOMAINS

1. Microsoft 365 Tenant Governance and Policy Management

- **Microsoft Purview Information Protection:** sensitivity label design, auto labeling policy authoring, encryption and rights management at scale
- **Purview Data Loss Prevention (DLP):** policy authoring across Exchange Online, SharePoint, OneDrive, Teams, and endpoints
- **Purview Records Management:** retention label policies, file plan administration, disposition review workflows
- **Purview Communication Compliance:** policy design for sensitive communication monitoring
- **Purview eDiscovery:** Standard and Premium configuration for legal hold and investigation workflows
- **Purview Audit (Standard/Premium):** audit log search, evidence collection, investigation
- **Microsoft 365 Admin Center:** tenant-level policy, license management, Secure Score, Compliance Manager

2. Identity, Access, and Privileged Access Governance

- **Microsoft Entra ID (Azure AD):** tenant configuration, hybrid identity federation, B2B/B2G external collaboration controls
- **Conditional Access:** policy authoring for risk based authentication, device compliance enforcement, location based controls, session controls via Defender for Cloud Apps
- **Privileged Identity Management (PIM):** just in time admin role activation, access reviews, eligible vs. active assignment governance
- **Identity Governance:** access reviews, entitlement management, lifecycle workflows
- **Administrative Units:** federated delegation for Major-Command style organizational structures
- **Microsoft Authenticator / FIDO2 / WHfB:** phishing-resistant MFA deployment, passwordless enrollment
- **Active Directory:** on premises AD, Group Policy, Kerberos, AD Connect / Entra Connect synchronization

3. Data Classification and Tagging at Enterprise Scale

- Automated classification using Purview's trainable classifiers and exact data match (EDM)
- Sensitive Information Type (SIT) authoring for organization specific data patterns
- Integration with file servers via Microsoft Information Protection scanner for hybrid environments
- Cross workload label policies (Exchange, SharePoint, OneDrive, Teams, Power BI, Power Platform)
- Auto classification + manual exception governance with periodic policy tuning and feedback loops

4. Records Management and Retention

- Retention label policies aligned to DoD Records Management Program requirements (DoDI 5015.02)
- File plan administration with regulatory record categorization
- Disposition workflows with custodian review and audit trails
- Hybrid retention coverage extending cloud retention labels to on premises content via Microsoft Information Protection scanner
- Litigation hold via Purview eDiscovery (Standard / Premium)

5. Security Operations and Threat Protection

- **Microsoft Defender for Endpoint:** policy tuning, threat hunting, automated investigation and response (AIR), attack surface reduction (ASR) rules
- **Microsoft Defender for Cloud Apps:** cloud app discovery, session control, conditional access app control
- **Defender Advanced Hunting:** threat hunting via Defender query language, anomaly investigation, alert tuning
- **Tier 3 incident response:** root cause analysis, containment, eradication, customer facing incident communications

- **Microsoft Secure Score / Compliance Manager:** tenant baseline assessment, control attestation, posture improvement roadmaps
- **KnowBe4:** phishing simulation, security awareness training campaigns, user-risk score tracking

6. Network Security and Perimeter Operations: Multi Vendor

Production hands on operations across the network security platforms that dominate federal civilian, DoD, SLED, and tribal IT environments:

- **Palo Alto Networks PAN-OS:** base NGFW policy design and configuration. (Palo Alto Networks is widely deployed across DoD networks under enterprise license arrangements.)
- **Cisco:** ASA firewalls, Firepower Threat Defense (FTD), ISR routers, AnyConnect VPN, Cisco UCS server platform. (Cisco dominates the install base across federal civilian agencies and IHS.)
- **Cisco Meraki:** MX security appliances, MS switches, MR access points, Systems Manager MDM, cloud managed dashboard. (Cisco Meraki is dominant in federal civilian remote sites, K-12, and county / state agencies; Meraki for Government holds FedRAMP Moderate authorization.)
- **Fortinet FortiGate:** NGFW policy design, VPN (IPsec / SSL), VDOM administration (multi tenant FortiGate), FortiManager / FortiAnalyzer, Security Fabric. (Fortinet leads SLED firewall renewals; Fortinet Federal Inc. provides DoDIN APL-approved variants for DoD work.)
- **FortiClient / FortiSwitch / FortiAP:** endpoint compliance, endpoint VPN, Security Fabric integration. (Fortinet ZTNA exposure is familiarity-level; primary ZTNA experience is via Entra ID Conditional Access.)
- **SonicWall:** TZ / NSa / NSsp series, Capture Security Center, Cloud App Security. (SonicWall is common in K-12, small county government, and small federal subcontractor environments.)
- **HPE Aruba:** Aruba switching and wireless production deployments, plus Aruba Central cloud managed networking dashboard. (HPE Aruba is heavily deployed across federal civilian agencies and SLED via NASPO + GSA contract vehicles.)
- **WatchGuard, Ubiquiti:** small business and remote office tier deployments.
- **Network segmentation and zoning:** defense in depth design across multi tenant regulated MSP environments.
- **Switch and routing operations:** VLAN, trunking, L3 policy, multi vendor migration projects (e.g., Cisco-to-Fortinet, Fortinet-to-Palo Alto, HPE Aruba-to-Cisco).

7. Virtualization and Datacenter Operations

- **VMware vSphere / vCenter / vSAN:** production hypervisor administration, HA cluster operations, datastore management, capacity planning, version uplifts
- **Microsoft Hyper-V:** clustering, live migration, production deployments at lower tier scale
- **Post-Broadcom virtualization strategy:** license impact analysis (VVF / VCF), Hyper-V migration evaluation, Veeam based DR continuity through migration windows
- **Datacenter operations:** server lifecycle management, SAN / RAID storage, infrastructure refresh leadership, end of support remediation, full server builds and rack deployments across MSP client environments
- **Server hardware:** HPE Synergy (composable infrastructure), Cisco UCS (Unified Computing System), HP / HPE rack servers, Dell servers
- **Storage:** HPE Nimble Storage, HPE 3PAR, NetApp, Synology, VMware vSAN. Fibre Channel, iSCSI, and direct-connect SAS connectivity
- **Backup and disaster recovery:** Veeam, Datto, Axcient, Dropsuite, Veritas, Microsoft 365 backup tooling, on prem to cloud DR design

8. Email Security and Hybrid Mail

- **Exchange Online:** mail flow, transport rules, anti-phishing, Safe Links, Safe Attachments
- **Hybrid Exchange:** on prem to cloud migrations, hybrid mail flow design, coexistence
- **Email authentication:** SPF, DKIM (multi-selector), DMARC reporting and policy progression, MTA-STS, BIMI considerations
- **DNSSEC-signed zones:** deployment, DS publication, zone-signing key rotation
- **Defender for Office 365:** ATP policies, attack simulator, threat explorer

9. Compliance Program Support: Translation to Federal Requirements

Framework Experience	Translation to Federal / DoD Requirements
HIPAA Security Rule	Risk analysis (164.308(a)(1)), access control (164.312(a)), audit controls (164.312(b)), evidence collection. Crosswalks to NIST SP 800-66r2 and NIST 800-53 (Moderate baseline). Audit evidence patterns translate to DoD CUI handling under NIST 800-171.
PCI DSS (v3.2.1 era hands on)	Network segmentation (Req 1), access control (Req 7-8), vulnerability management (Req 5-6, 11), audit logging (Req 10). Crosswalks to NIST SP 800-171 / CMMC Level 2 control families AC, AU, CM, SC, SI.
CJIS Security Policy v6 (SEPP)	Multi state law enforcement client support. CJIS Security Policy Appendix G provides direct crosswalk to NIST SP 800-53 controls. Advanced Authentication, audit logging, and physically secure location requirements translate to NIST 800-171 control families.
FFIEC / GLBA (banking)	No direct GLBA / FFIEC examination work. Adjacent regulatory rigor pivot from PCI DSS and HIPAA experience: same evidentiary, control design, and audit readiness patterns. FFIEC Cybersecurity Assessment Tool (CAT) and Information Security IT Examination Handbook align with NIST CSF and NIST 800-53.
NIST CSF / 800-53	General familiarity for cyber program design across Identify / Protect / Detect / Respond / Recover function categories.

These regulatory patterns share evidentiary, control design, audit readiness, and continuous monitoring requirements with NIST 800-53 Moderate, NIST 800-171 / CMMC Level 2, and DoD CUI handling under DoDI 5200.48.

10. Microsoft Cloud Partner and Licensing

- **Microsoft 365 / Office 365 licensing:** EA, CSP, NCE evaluation; SKU-to-feature mapping for compliance contexts
- **Microsoft 365 Business Basic / Business Standard / Business Premium:** tenant deployment, custom domain federation, MX / SPF / DKIM / DMARC integration
- **Microsoft Cloud Partner Program:** evaluating enrollment ahead of CSP eligibility

Live Security Posture (Walk the Walk)

Soulier Group LLC operates this website with the same defense in depth posture we recommend to clients. **HTTP controls:** HSTS preload, strict Content Security Policy, X-Frame-Options DENY, Referrer-Policy strict-origin-when-cross-origin, Permissions-Policy lockdown. **DNS:** DNSSEC signed (DS at .com TLD, ECDSA P-256 / SHA-256). **Mail:** SPF hard fail, DKIM 2-selector, DMARC published. **Federal alignment:** approach mirrors OMB M-21-07 IPv6-readiness expectations and CISA BOD 18-01 mail authentication requirements. Independent verification welcome via the `security.txt` at /.well-known/security.txt.

DIFFERENTIATORS FOR PRIME SUBCONTRACTING TEAMS

1. **DoD 8140 IA Level II baseline (Active CompTIA Security+ SY0-701):** principal holds the federally recognized cybersecurity workforce qualification (achieved 2026-05-10); satisfies "Sec+ or equivalent" prerequisite common in DoD and civilian federal IT solicitations.
2. **ISBEE / SDB certified small business:** provides socioeconomic credit on prime evaluation criteria for federal solicitations.
3. **Production Microsoft 365 multi tenant administration experience:** direct production responsibility across regulated client portfolios, not academic exposure.
4. **Lean operational profile:** single accountable owner pattern reduces bench management overhead for primes; ideal for smaller named sub roles or specific labor categories.
5. **Cross domain compliance experience:** HIPAA + PCI + CJIS breadth is uncommon in single practitioners; useful for primes presenting compliance driven proposals.
6. **Native American Owned, ISBEE certified:** supports federal tribal preference and minority business participation goals.
7. **Microsoft Cloud Partner Program:** evaluating enrollment ahead of CSP eligibility milestones.
8. **Federal procurement cycle literacy:** Army DTSPO M365 Records Management RFI submitted May 2026; ongoing Sources Sought / RFI monitoring across primary NAICS. Reads PWS documents and writes federal-grade technical responses.

ENGAGEMENT AVAILABILITY

- **Labor categories:** Senior Microsoft 365 Engineer, Senior Cyber Engineer, Senior Network Security Engineer, Senior Systems Engineer, Compliance Engineer, Microsoft Purview Specialist, Virtualization / VMware Engineer
- **Engagement model:** 1099 subcontractor at prime's labor rates, FFP task assignments, or Time-and-Materials
- **Availability:** Immediate
- **Facility Clearance (FCL):** None held. **Personnel Clearance (PCL):** US citizen; eligible for clearance sponsorship at applicable levels per investigation findings.