

Policy & Documentation Development Intake Guide

Thank you for booking a Policy & Documentation Development session with Resilience Cyber Group. This guide will help you prepare in advance so we can maximize the value of your session.

Company & Contact Information

- Legal company name
- Primary contact (name & title)
- Work email & phone
- DUNS/UEI (if applicable)

Contract & Data Context

- Do you handle Controlled Unclassified Information (CUI)?
- Applicable clauses/standards (DFARS, NIST SP 800-171, CMMC 2.0, ITAR, etc.)
- Prime contractor / Contract identifier (if available)

Environment & Boundaries

- Where is the in-scope environment hosted? (On-prem, GCC, GCC High, AWS Gov, etc.)
- Approximate user count in scope
- System boundary summary (core IT systems, email, file share, endpoints, etc.)

Documentation Status

- Current SSP status (none, draft, near-final, maintained)
- Policies and procedures currently available
- Where documents are stored (SharePoint, OneDrive, Confluence, etc.)

External Partners & Tools

- MSP/MSSP or key vendors supporting your IT/security environment
- Security tooling in use (EDR, SIEM, vulnerability management, MDM, etc.)

Compliance Posture & Evidence

- SPRS score (if any) and assessment date
- Top 3 cybersecurity risks or pain points
- Evidence workflows today (ad-hoc, defined, routine, audited)

Scope & Scheduling

- Priority deliverables for this engagement (SSP, policy refresh, POA&M, etc.)
- Target timeline (2–4 weeks, 4–8 weeks, etc.)
- Other notes/constraints (blackout dates, availability, etc.)

Please email existing policies, SSP drafts, or documentation repositories to **info@rcybergroup.com** prior to your session. This preparation will allow us to accelerate your compliance journey and deliver actionable outputs more efficiently.