DIB Collective Eligibility Requirements & Membership Expectations

Purpose of Membership

The DIB Collective is specifically intended to represent Organizations Seeking Certification (OSCs) and other Defense Industrial Base organizations when approved by the Chair that are directly responsible for implementing, maintaining, and operating under cybersecurity, contractual, and compliance requirements.

The purpose of the DIB Collective is to ensure that the organizations beholden to these requirements have a direct and meaningful voice in the broader CMMC and cybersecurity conformity ecosystem.

Members should bring the perspective of organizations that must translate cybersecurity and compliance requirements into actual business operations, including the organizations that must budget for implementation, modify systems and processes, train employees, manage suppliers, protect information, prepare for assessments, maintain compliance, and address the operational consequences of evolving requirements.

The DIB Collective is not intended to duplicate stakeholder forums representing cybersecurity service providers, consultants, assessors, or other organizations whose primary role is advising, assessing, selling to, or supporting OSCs.

Organizational Eligibility

To be eligible for membership in the DIB Collective, an applicant should represent an organization that:

1. **Operates within the Defense Industrial Base or directly supports the performance of government or defense-related contracts** as a contractor, subcontractor, supplier, manufacturer, engineering organization, technology company, or other organization subject to applicable cybersecurity or information-protection requirements; and

2. **Is an Organization Seeking Certification (OSC), expects to become an OSC, or is otherwise directly responsible for implementing and maintaining cybersecurity and compliance requirements within its own organization; and**

3. **Has practical experience implementing or preparing to implement requirements** such as CMMC, NIST SP 800-171, DFARS cybersecurity requirements, FAR cybersecurity requirements, or other applicable federal cybersecurity and information-protection obligations; and

4. **Can contribute practical insight regarding the cost, complexity, operational impact, implementation challenges, unintended consequences, and effectiveness** of cybersecurity and compliance requirements within an operating DIB organization; and

5. **Is willing to participate constructively**, share practical experience where appropriate, respect differing viewpoints, and support the mission and objectives of the DIB Collective.

Primary-Business-Model Limitation

The DIB Collective is specifically intended for the companies that must **implement the requirements, pay for them, integrate them into day-to-day operations, and live with their practical consequences.**

Accordingly, if an organization's **primary business model is providing cybersecurity, compliance, consulting, assessment, certification, managed services, or similar professional services to other businesses**, the DIB Collective is generally not intended to be that organization's stakeholder forum.

This includes organizations whose principal business is providing services such as:

- CMMC assessments or certification services;
- Cybersecurity or compliance consulting;
- Managed IT or managed security services;
- CMMC implementation or readiness services;
- Compliance documentation or advisory services;
- Cybersecurity products or platforms where participation would primarily represent the interests of a vendor or service provider; or
- Similar commercial services primarily marketed to OSCs or other DIB organizations.

This limitation is not intended to suggest that these organizations are not important participants in the CMMC ecosystem. Their expertise and perspectives are valuable and may be represented through other Cyber EF Stakeholder Council groups, invited subject-matter-expert participation, joint discussions, or other appropriate forums.

Rather, **the DIB Collective is intentionally designed to preserve a distinct voice for the organizations on the receiving end of cybersecurity and compliance requirements.**

The broader ecosystem, including Cyber EF, The Cyber AB, government stakeholders, assessors, consultants, service providers, and policymakers, needs a clear understanding of how requirements work from the perspective of the organizations actually beholden to the rules.

Eligibility Based on the Organization Represented

Eligibility should be based primarily on the organization and perspective the individual represents within the DIB Collective, rather than solely on the individual's professional credentials or cybersecurity expertise.

An individual employed by an eligible OSC or DIB organization does not need to work in cybersecurity or compliance to participate. Executives, owners, operations leaders, manufacturing leaders, IT and cybersecurity personnel, quality professionals, contracts professionals, supply-chain personnel, engineers, and other employees may provide valuable perspectives regarding the practical effects of cybersecurity and compliance requirements.

Conversely, an individual's personal experience working with OSCs does not by itself establish eligibility when that individual's organization primarily derives its business from selling cybersecurity, compliance, assessment, consulting, or managed services to OSCs.

Exceptions and Invited Participation

The Chair may invite cybersecurity professionals, assessors, consultants, government representatives, attorneys, subject-matter experts, technology providers, or other ecosystem participants to attend particular meetings, working sessions, committees, or discussions when their expertise would benefit the DIB Collective.

Such invited participation does not necessarily constitute membership or alter the Collective's primary purpose of representing OSC and DIB operator perspectives.

The Chair may also approve membership in exceptional circumstances where an applicant does not fit neatly within these criteria but brings a perspective that is materially important to the mission of the DIB Collective and does not undermine the Collective's role as the voice of organizations responsible for implementing and operating under the requirements.

Member Expectations

Membership in the DIB Collective is a participatory role, not a permanent designation. Continued membership is dependent upon maintaining eligibility and may also be conditioned upon reasonable attendance, participation, and conduct requirements established by the Chair consistent with the DIB Collective Charter.

Members are expected to:

- Represent the practical experiences and interests of OSCs and DIB organizations in good faith;
- Participate regularly and prepare for meetings and working-group activities;
- Contribute candid, constructive, and solution-oriented feedback;
- Distinguish personal or organizational commercial interests from broader OSC and DIB concerns;
- Disclose material conflicts of interest when appropriate;
- Refrain from using DIB Collective participation primarily for sales, lead generation, marketing, or promotion of commercial products or services;
- Respect confidentiality and all applicable information-handling requirements;
- Avoid introducing CUI, classified information, export-controlled technical data, proprietary third-party information, or other restricted information into Collective activities; and
- Abide by applicable Cyber EF professional conduct requirements and the DIB Collective Charter.

Committee and Working Group Lead Expectations

Serving as a Committee or Working Group Lead is a leadership role within the DIB Collective and carries additional responsibilities beyond those expected of general members. Leads should be prepared to actively organize, communicate, and advance the work of their group.

Committee and Working Group Leads are expected to:

- **Communicate regularly and clearly** with committee or working group members, the DIB Collective Chair, and other DIB Collective leadership as appropriate.
- **Maintain momentum between meetings**, including communicating next steps, following up on action items, coordinating member contributions, and identifying issues that may require additional support or direction.
- **Provide regular updates on the group's activities and progress.** This may include meeting summaries, status reports, key findings, recommendations, upcoming priorities, identified challenges, or other information needed to maintain visibility into the group's work.
- **Attend the monthly DIB Collective Leadership meeting** and be prepared to provide updates, raise issues requiring broader discussion, coordinate with other committees or working groups, and participate in Collective-wide planning and prioritization.
- **Plan and facilitate committee or working group meetings**, including establishing agendas, identifying priorities, assigning or coordinating action items, and helping ensure that meetings result in meaningful progress.

- **Coordinate deliverables and work product** developed by the group and communicate regularly with the Chair regarding significant recommendations, findings, concerns, or proposed external communications.
- **Encourage active and constructive participation** from members while ensuring that the work of the group remains consistent with its assigned scope and the mission of the DIB Collective.
- **Promptly communicate obstacles or concerns** that could materially affect the group's progress, participation, deadlines, or ability to complete its work.

Prospective Leads should understand that the time commitment associated with these roles will vary considerably depending upon the committee, current projects, deadlines, and activity within the CMMC and broader cybersecurity ecosystem. During periods of significant activity, a Committee or Working Group Lead may devote approximately **five to ten (5–10) hours per week** to DIB Collective responsibilities, including meetings, communications, coordination, preparation, and development or review of work product.

Individuals accepting a Lead role should do so with the understanding that **consistent communication, responsiveness, and follow-through are essential to the position.** If a Lead is temporarily unable to devote the time necessary to effectively support the group, the Lead should communicate with the Chair so that responsibilities, timelines, or leadership coverage can be adjusted as appropriate.