DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program Framework Agreement Amendments

All companies that participate in DoD's DIB CS Program must have a Framework Agreement (FA) on file with DoD, which formalizes the information sharing relationship between a company and DoD.

When DoD and the DIB share cyber threat information bilaterally, both parties can better anticipate and identify malicious cyber activity, bolstering threat mitigation actions.

The DIB CS Program has four optional Amendments to the FA for participating Companies to further promulgate cybersecurity information in support of a more resilient DIB: Subsidiary, International Business Unit (IBU), Third-Party Service Provider (TPSP), and Supply chain.

Subsidiary Amendment

- Allows a participating company to share unclassified Government Furnished Information (GFI) with wholly-owned subsidiaries that also meet the eligibility requirements of the DIB CS Program.
- Authorizes the DIB CS Program participant to share unclassified GFI with its Subsidiary(ies) or apply unclassified GFI to the Subsidiary(ies)'s U.S. based information systems.
- A Subsidiary is any company that is owned and controlled by the DIB CS Program participant (i.e., the FA signatory) and that meets the eligibility requirements of Title 32 of Code of Federal Regulations, Part § 236.7.
- Subsidiaries may report cyber incidents and indicators either directly to the Government or through its parent company.

International Business Unit Amendment

- Allows a participating company to share unclassified GFI with business units located in the UK, Australia, New Zealand, and Canada.
- Authorizes sharing of unclassified GFI extracts by DIB CS Program participant with its designated IBUs located in covered county(ies).
- An IBU can be the parent company of a participating company, a corporate division, a wholly-owned subsidiary, or other legal entity under the control of the DIB CS Program participant.
- IBUs may report cyber incidents and indicators either directly to the Government or through its parent company.

OSD.DIBCSIA@mail.mil
https://DIBNet.dod.mil
(703) 604-3167

@DoD_CIO
linkedin.com/in/dod-cio

Third-Party Service Provider Amendment

- Enables a participating company to share unclassified GFI with a third-party service provider (TPSP) providing information security services support to the company.
- DIB CS Program participants who employ a TPSP are authorized to share DIB CS unclassified GFI with the designated TPSP for the purpose of providing information security services support for the DIB CS Program participant.
- The DIB CS participant must indicate whether the TPSP will provide on-site or off-site support, how the TPSP will access the GFI, and who will report cyber incidents and indicators to the Government.

Supply Chain Amendment

- Allows a participating company to share unclassified GFI with designated supply chain participants and leverage a capability to help identify adversarial activity on their supply chain networks.
- The Company may use unclassified GFI extracts with the Company's designated supply chain participants for the purpose of providing information security services to assist and identify adversary activity affecting such supply chain participants.
- Cyber incidents and indicators detected by the company in connection with installation of the capability and use of GFI will be reported to DoD in accordance with the FA.
- The term "capability" in the context of this amendment refers to hardware or software applied physically or remotely, in order to passively or actively monitor outbound network traffic, and includes built-in technology allowing for communication to a remote administrator over an encrypted communication channel.

LEARN MORE

More information about the DIB CS Program can be found on our website, DIBNet, at https://dibnet.dod.mil

VISIT US

OSD.DIBCSIA@mail.mil
https://DIBNet.dod.mil
(703) 604-3167

@DoD_CIO
linkedin.com/in/dod-cio