DIB CyberDome™

Protecting Small and Medium Defense Contractors from Modern Cyber Threats

THE PROBLEM

Across the Defense Industrial Base, thousands of small and medium-sized contractors support critical U.S. defense systems, managing sensitive technical data, production specifications, and operational processes tied directly to national security.

These organizations are increasingly targeted by sophisticated cyber adversaries, but lack the resources, personnel, and infrastructure required to defend themselves effectively. This risk has intensified in the current geopolitical environment, including increased cyber activity associated with Iranian state-affiliated groups following Operation Epic Fury.

Unlike large defense contractors with dedicated SOC teams, SIEM platforms, and extensive cybersecurity investments, most operate with limited staff, constrained budgets, and fragmented tools.

The result: high-value targets with limited capacity to defend against modern threats.

CELERIUM.com

©2026 Celerium, Inc. All Rights Reserved

A DIFFERENT APPROACH

DIB CyberDome™ introduces a purpose-built model for small and medium members of the Defense Industrial Base.

At its core is the Cyber Interceptor, designed to:

- **Intercept threats before they enter contractor systems**
- **Continuously adapt to changing threat conditions**
- **Operate effectively without heavy operational burden**

It is a system designed for busy contractors with little or no IT security staff.

BUILT FROM DEFENSE INDUSTRIAL BASE OPERATIONAL EXPERIENCE

DIB CyberDome™ is derived from Celerium's operational experience supporting small and medium defense contractors through its **DCISE³ solution**, which has been made available to eligible contractors through the **DC3 DCISE program within the Defense Industrial Base (DIB) Cybersecurity (DIB CS) initiatives.**

Operating at scale across the Defense Industrial Base, this experience reflects how contractors manage sensitive systems while facing continuous threat activity with limited resources.

The **Cyber Interceptor builds directly on this foundation**, translating real-world DIB operating conditions into a system designed to intercept threats before they enter contractor environments and continuously adapt to changing threat activity.

HOW IT WORKS: INDIVIDUAL DEFENSE AND COLLECTIVE STRENGTH

DIB CyberDome™ combines:

- **Individualized protection for each contractor**
- **Shared insight across the Defense Industrial Base**

©2026 Celerium, Inc. All Rights Reserved

Each participant benefits from both their own protection and broader ecosystem awareness and threat intelligence.

INDIVIDUAL PROTECTION

For each organization, the Cyber Interceptor delivers adaptive protection:

CONTINUOUS THREAT ADAPTATION

Defensive controls are automatically re-optimized, typically every 15 minutes, to respond to evolving threat activity.

ENVIRONMENT-AWARE PROTECTION

Protection is aligned to each organization's infrastructure, including hybrid on-prem and cloud environments.

CONFIGURABLE DEFENSE LEVELS

Organizations define their level of protection based on operational needs and risk tolerance.

IMPLEMENTATION, ENGINEERED FOR REAL-WORLD DEPLOYMENT

- No hardware or appliances required
- No endpoint agents or EDR deployment
- No packet inspection required
- Deploys through existing perimeter firewalls
- Securely sends metadata to a decision engine within **AWS Government Cloud infrastructure**
- Typical implementation: **30–60 minutes**

BUILT FOR TODAY'S THREAT ENVIRONMENT, INCLUDING IRAN-DRIVEN CYBER ESCALATION

The current threat environment is being shaped by active geopolitical conflict.

Following the launch of Operation Epic Fury on February 28, 2026, cyber operations have become tightly integrated with military activity, with coordinated cyber and kinetic campaigns executed in parallel.

In response, Iranian state-affiliated and aligned groups have escalated cyber operations, shifting toward coordinated and disruptive campaigns targeting U.S. and allied organizations, including elements of the Defense Industrial Base.

©2026 Celerium, Inc. All Rights Reserved

These campaigns generate rapidly evolving threat indicators, including infrastructure, behavioral patterns, and attack signatures associated with Iranian cyber operations.

The Cyber Interceptor has incorporated Iranian based threat indicators, updating defensive controls in near real time to block adversary activity before it reaches contractor systems.

Small and medium defense contractors, often outside traditional defense perimeters, are increasingly exposed to this activity.

DIB CyberDome™ is designed for this environment, combining continuously updated threat intelligence with automated interception and adaptive defense.

DIB CyberDome™

A new model for protecting the Defense Industrial Base, built from real operational experience and designed for how it actually operates.

CELERIUM.com

©2026 Celerium, Inc. All Rights Reserved