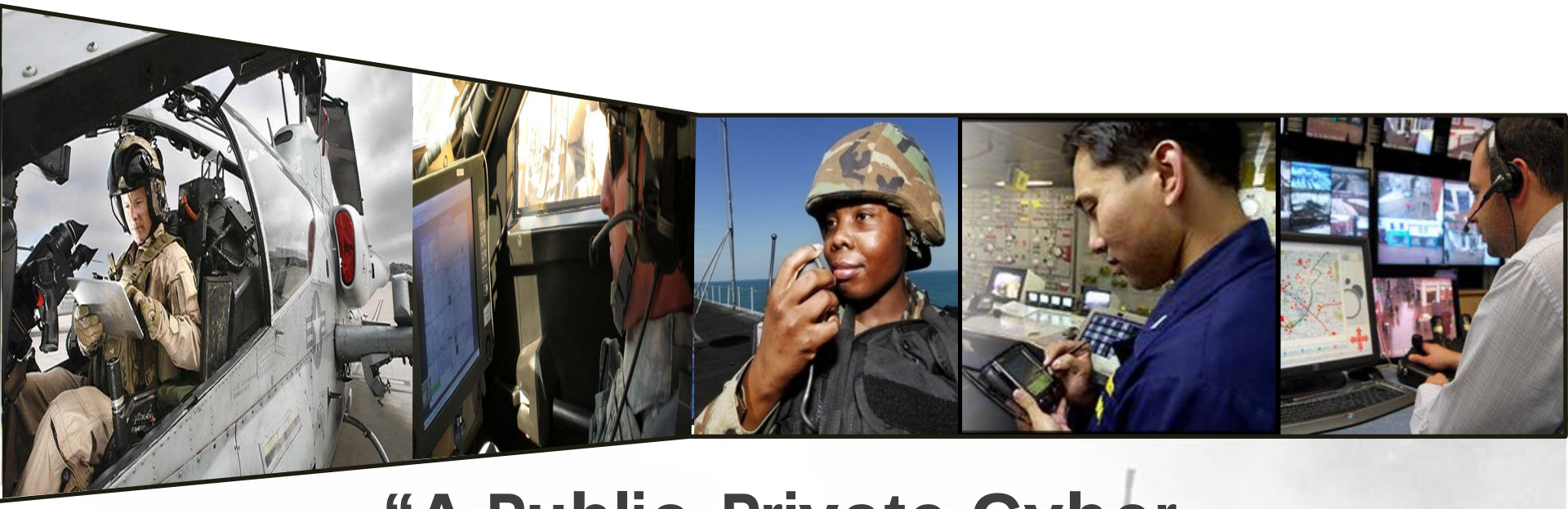
DoD's DIB CS/IA Program



"A Public-Private Cyber Security Partnership"

April 22, 2014

DIB CS/IA Program

Mission Statement

The Deputy Secretary of Defense directed the establishment of the DIB CS/IA program in 2007 under DoD CIO.

DIB CS/IA Mission

To enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

DIB CS/IA Program

Authorities

- DIB CS/IA activities, including the collection, management and sharing of information for cyber security purposes, support and implement the following national and DoD-specific guidance and authority:
  - DoD CIO 10 U.S.C. § 2224
  - Federal Information Security Management Act (FISMA) (44 U.S.C. §§ 3541 et seq.)
  - PPD-21: Critical Infrastructure Security and Resilience. Replaces HSPD-7. DoD is the sector-specific agency for the DIB.
  - Part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities" of title 32, Code of Federal Regulations (CFR), 22 Oct 2013.

DIB CS/IA Program

Program Objectives

DoD and DIB Partners share a mutual concern regarding the security of critical DoD unclassified information that resides on, or transits, DIB unclassified information systems. DIB CS/IA Program objectives follow:

- Establish a voluntary, mutually acceptable framework to protect information from unauthorized access
- Create a trusted environment to maximize network defense and remediation efforts by:
  - Sharing cyber threat information and incident reports
  - Providing mitigation/remediation strategies and malware analysis
  - Assessing damage to defense programs/technology from suspected compromises
- Protect the confidentiality of information exchanged to the maximum extent authorized by law
- Increase USG and DIB knowledge of adversary

DIB CS/IA Program

DIB CS/IA Program Eligibility

A cleared defense contractor must:

- Have DoD-approved medium assurance certificates
- Have an existing facility clearance with approved safeguarding to at least the Secret level
  - Companies in DIB CS/IA application process may be sponsored for Safeguarding at the Secret level
- Have or acquire a Communication Security (COMSEC) account
- Obtain access to DoD's secure voice and data transmission systems supporting the DIB CS/IA program
- Own or operate covered DIB system(s)
- Execute the standardized Framework Agreement

DIB CS/IA Program

Program Elements

- Framework Agreement
- Information Sharing
- Reporting and Response
- Damage Assessment
- DIB Enhanced Cyber Security Services (DECS)

DIB CS/IA Program

DIB Enhanced Cyber Security Services

- DECS, an optional component of DIB CS/IA program
  - Jointly managed capability between DoD and DHS
  - Provides another layer of protection for DIB participants
- DIB companies may elect to participate in DECS in one of three ways:
  - Customer: Receive services from a supporting DHS-approved Commercial Service Provider
  - Operational Implementer: Directly receive classified threat indicators
  - CSP: As a DHS-approved CSP offer services to other DIB participants
- The Government will furnish classified cyber threat and technical information either to a DIB company or to the DIB company's Commercial Service Provider (CSP).
  - Enables these DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of known malicious cyber activity.

DIB CS/IA Program

DFARS Safeguarding Unclassified Controlled Technical information

- **Defense Federal Acquisition Regulations Supplement (DFARS) Clause 252.204-7012,**
  - Clause posted and effective November 18, 2013
  - A contractual requirement
  - Mandates certain network security safeguards to protect DoD unclassified controlled technical information
  - Mandates reporting of cyber incidents that may have affected DoD unclassified controlled technical information

Section 941 National Defense Authorization Act (NDAA) for FY13

- **Section 941 National Defense Authorization Act (NDAA) for FY 13**
  - Applies to all Cleared Defense Contractors (CDCs)
  - Mandates reporting of each successful penetration of CDC network or information system(s):
    - A description of the technique or method used in such penetration(s).
    - A sample of the malicious software, if discovered and isolated by the contractor, involved in such intrusion(s).
    - A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration(s).
  - CDCs must provide DoD access to equipment or information to determine what DoD information was impacted
  - DoD will protect trade secrets, commercial or financial information, and personally identifiable information (PII)
    - DoD will not share sensitive information reported by a CDC, or derived from such reported information, outside of DoD without the permission of the reporting CDC.

DIB CS/IA Program

Contact Information

DIB CS/IA Program:

E-mail: OSD.DIBCSIA@mail.mil

Phone: (703) 604-3167

Toll Free Number: 1-855-363-4227

FAX: (703) 604-4745

http://dibnet.dod.mil