DoD CISO Special Session Town Hall

Feb 10, 2022 3-4pm EST

UNCLASSIFIED

DoD CISO Special Session Town Hall

February 10, 2022 from 3:00pm - 4:00pm ET

UNCLASSIFIED

Agenda

- Introductions
- DIB Cybersecurity Placemat
- CMMC
- USD(P)
- NSA CCC
- DC3/DCISE
- Q&A
- Closing Remarks

CURRENT DOD DIB CYBERSECURITY EFFORTS

CYBER THREAT INFORMATION/ INTELLIGENCE SHARING WITH DIB

- ***DoD CISO/DIB CS Program*** – voluntary public-private cybersecurity partnership between DoD and DIB to share information/intelligence; manages intel sharing platform, hosts events, maintains comms, and enables info/intel sharing
- ***DC3/DCISE*** **–** operational arm of DIB CS Program, sharing cyber threat info/intelligence, products, and tools to assist DIB
- ***NSA*** – shares "left of boom" products and tools with DIB
- ***USD(P)*** – PPD-21 DIB Sector Risk Management Agency

INCIDENT REPORTING

- ***DoD CISO/DIB CS Program*** – Oversight of DFARS 252.204-7012*; management of platform for voluntary and mandatory reporting; enables efforts to assess damage to DoD programs
- ***DC3/DCISE*** – single clearinghouse for unclassified Mandatory Incident Reports (MIR) per DFARS -7012; provides crowd-sourced, non-attributional reports to DIB on cyber threat information received from MIRs and voluntary reports
- ***DCSA*** – single clearinghouse for classified incident reports

DFARS 252.204-7012 ("DFARS-7012") stipulates a contractor's requirement to rapidly report cyber incidents within 72 hours of discovery at https://dibnet.dod.mil (DIBNet) and protect CUI.

DIB CYBERSECURITY REQUIREMENTS & ASSESSMENT MECHANISMS

- ***DoD CISO/DIB CS Program*** **–** assistance to DIB in understanding regulatory requirements
- ***DCMA*** – Oversight of DFARS 252.204-7019/7020*, DIBCAC
- ***DoD CIO*** – Oversight of DFARS 252.204-7021*, CMMC

DFARS 252.204-7019/7020 stipulates a contractor's requirement to implement NIST SP 800-171, have an assessment (basic, medium, or high), and prove ability to protect CUI.

DFARS 252.204-7021 stipulates a contractor have current CMMC certificate at the CMMC level required by the contract, and maintain the certificate at the required level for the duration of the contract.

CYBERSECURITY TECHNICAL ASSISTANCE AND COLLABORATION

- ***DoD CISO/DIB CS Program*** **–** offers vehicle for DoD collaboration with DIB, establishing and or maintaining relationships; hosts events, sub-working groups, and forums for collaboration
- ***DC3/DCISE*** – direct support to DIB through cost-free service offerings including: products, tools, strategies, and events
- ***NSA*** – targeted support to top-tier DIB for companies categorized as critical infrastructure

Additional official DoD policy/guidance is required to clearly assign all DIB roles and responsibilities

Cyber Threat Info/Intel Sharing with the DIB

DoD CISO/DIB CS Program

- Voluntary public-private cybersecurity partnership between DoD and DIB to share information/intelligence
- Manages intel sharing platform, hosts events, maintains comms, and enables information/intelligence sharing

DC3/DCISE

- Operational arm of DIB CS Program, sharing cyber threat info/intelligence, products, and tools to assist DIB

NSA

- Shares “left of boom” products and tools with DIB

USD(P)

- PPD-21 DIB Sector Risk Management Agency

Incident Reporting

DoD CISO/DIB CS Program

- Oversight of DFARS 252.204-7012*
- Management of platform for <u>voluntary</u> and mandatory reporting; enables efforts to assess damage to DoD programs

DC3/DCISE

- Single clearinghouse for unclassified Mandatory Incident Reports (MIR) per DFARS -7012
- Provides crowd-sourced, non-attributional reports to DIB on cyber threat information received from MIRs and <u>voluntary</u> reports

DCSA

- Single clearinghouse for classified incident reports

****DFARS 252.204-7012 (“DFARS-7012”) stipulates a contractor’s requirement to rapidly report cyber incidents within 72 hours of discovery at <u>https://dibnet.dod.mil</u> (DIBNet) and protect CUI.***

DIB Cybersecurity Requirements & Assessment Mechanisms

DoD CISO/DIB CS Program

- Assistance to DIB in understanding regulatory requirements

DCMA

- Oversight of DFARS 252.204-7019/7020*, DIBCAC

DoD CIO

- Oversight of DFARS 252.204-7021*, CMMC

****DFARS 252.204-7019/7020 stipulates a contractor's requirement to implement NIST SP 800-171, have an assessment (basic, medium, or high), and prove ability to protect CUI.***

****DFARS 252.204-7021 stipulates a contractor have current CMMC certificate at the CMMC level required by the contract, and maintain the certificate at the required level for the duration of the contract.***

Cybersecurity Technical Assistance & Collaboration

DoD CISO/DIB CS Program

- Offers vehicle for DoD collaboration with DIB establishing and or maintaining relationships
- Hosts events, sub-working groups, and forums for collaboration

DC3/DCISE

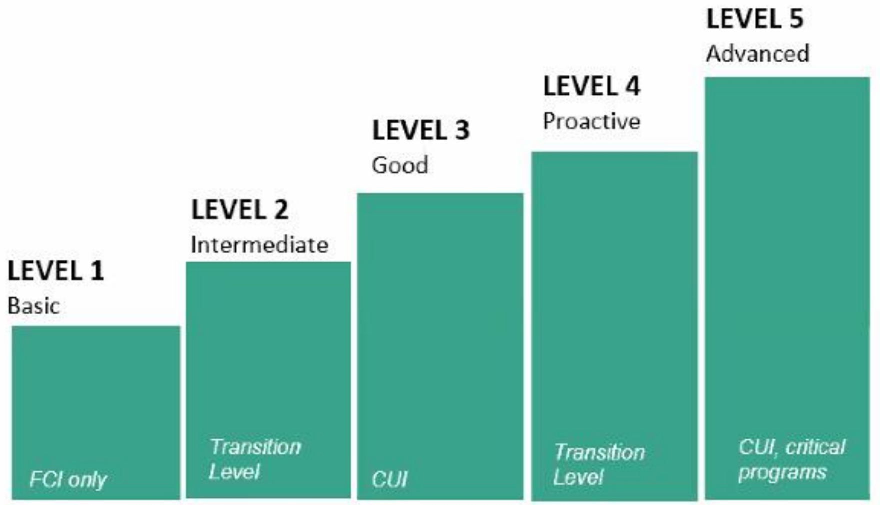
- Direct support to DIB through cost-free service offerings including: products, tools, strategies, and events

NSA

- Targeted support to top-tier DIB for companies categorized as critical infrastructure

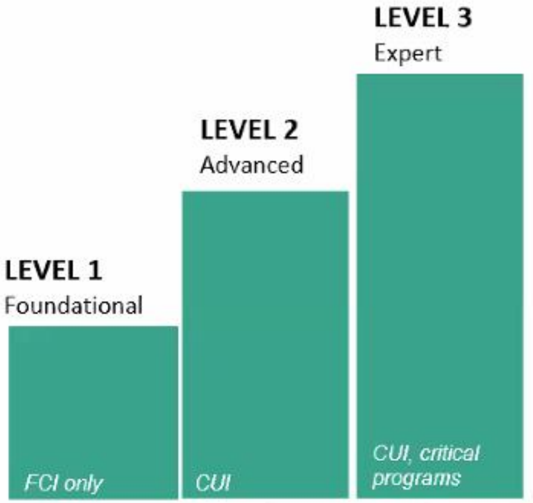
Streamlining CMMC

CURRENT FRAMEWORK: CMMC 1.0



	LEVEL 1 Basic	LEVEL 2 Intermediate	LEVEL 3 Good	LEVEL 4 Proactive	LEVEL 5 Advanced
	FCI only	*Transition Level*	*CUI*	*Transition Level*	*CUI, critical programs*
Model	17 practices	72 practices 2 maturity processes	130 practices 3 processes	156 practices 4 processes	171 practices 5 processes
Assessment	Third-party	None	Third-party	None	Third-party
Other					

REVISED FRAMEWORK: CMMC 2.0



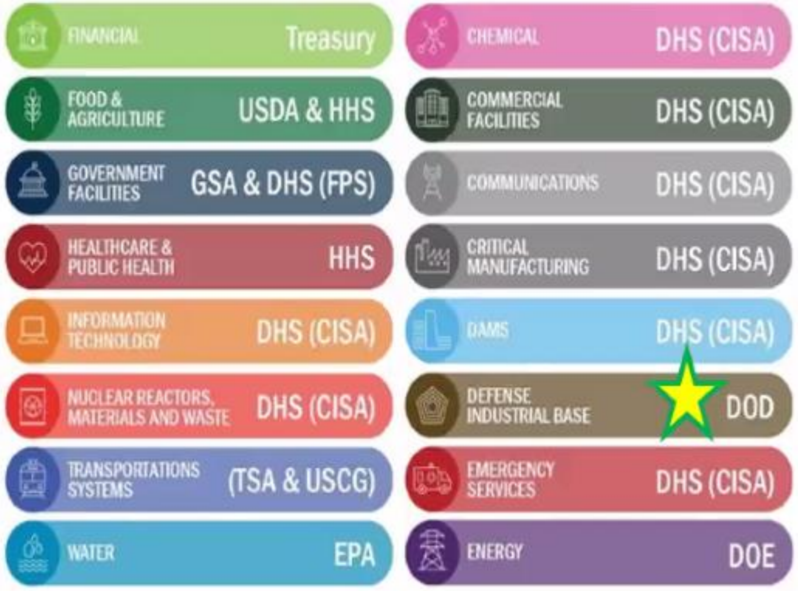
LEVEL 1 Foundational	LEVEL 2 Advanced	LEVEL 3 Expert
FCI only	*CUI*	*CUI, critical programs*
17 practices	110 practices based on NIST SP 800-171	110+ practices based on NIST SP 800-172
Self-Assessment	Third Party Assessments for critical national security information; self-assessment for select programs	Gov't-led Assessments
	POA&Ms and Waivers	POA&Ms and Waivers

USD(P)

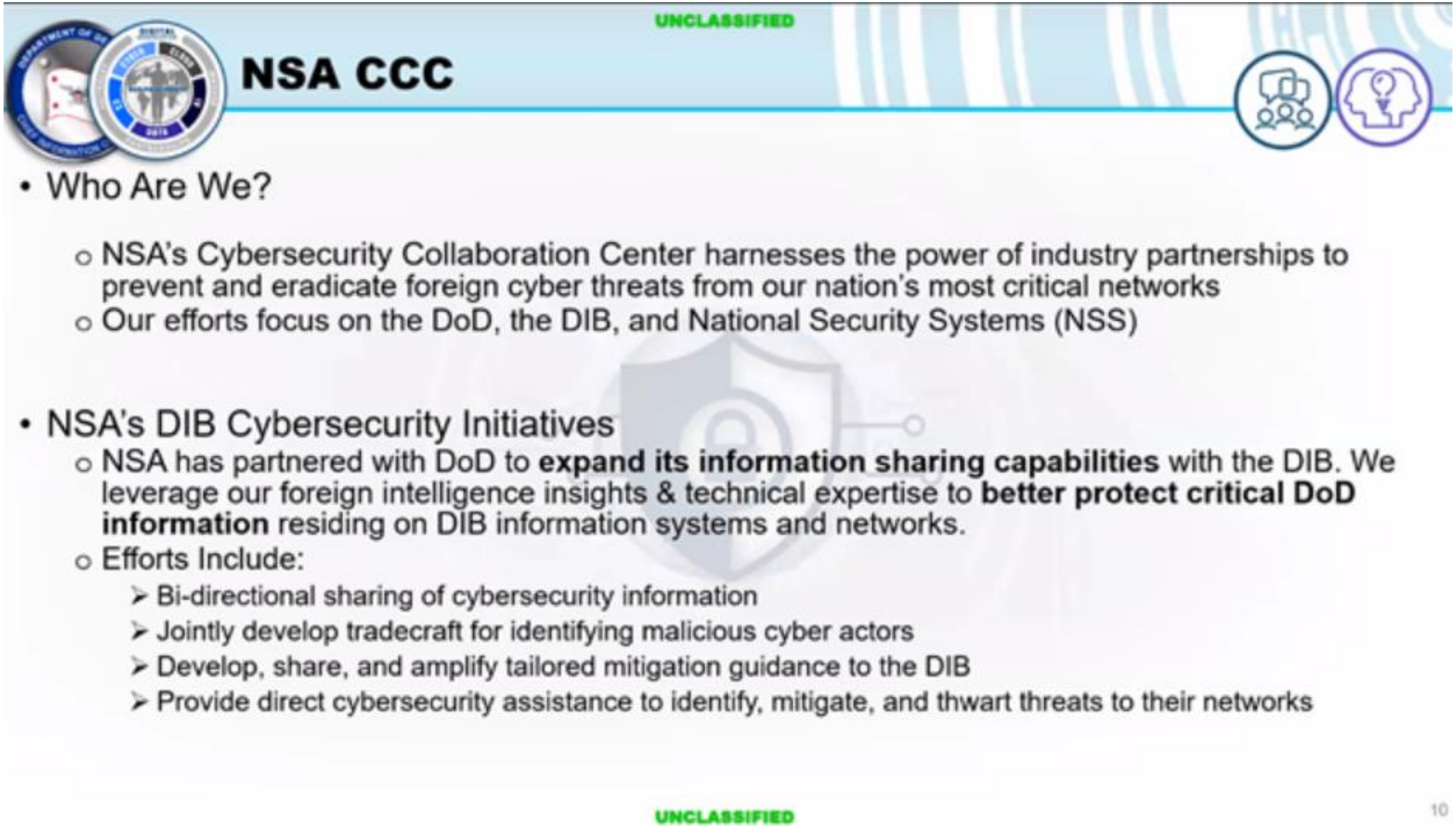
PPD-21 "Critical Infrastructure Security & Resilience" (2013)

- PPD-21 establishes 16 U.S. critical infrastructure sectors--including the DIB, communications, transportation, energy, and water– and directs the government to build trusted public-private partnerships to ensure secure, functioning, and resilient critical infrastructure.
  - Requires all threats and hazards to be considered.
- Designates DoD (Policy) as the DIB Sector Risk Management Agency (SRMA). USD(P) convenes and coordinates with partners across DoD, with the interagency, and private sector partners to:
  - Improve information and intelligence sharing with private sector partners;
  - Manage sector risks using public-private partnership efforts; and
  - Pursue sector critical incident and vulnerability management efforts.
- PPD-21 structure includes a Government Coordinating Committee (GCC), a private Sector Coordinating Committee (SCC), and Joint GCC-SCC Meetings. The National Defense-Information Sharing and Analysis Center (ND-ISAC) is the official ISAC for the DIB Sector.
  - ND-ISAC offers DIB Sector companies and their suppliers a community and forum for sharing cyber and physical security threat indicators, best practices, and mitigation strategies.
- DIB GCC priority efforts include DSD-endorsed tasks: 1) developing a framework for a cyber-secure DIB with the SCC; 2) establishing an "all-points bulletin" type messaging mechanism; and 3) updating Departmental cybersecurity requirements, roles, and responsibilities.
- USD(P) works with GCC and SCC partners to facilitate and support information sharing:
  - CIO's DoD-DIB CS Partnership (~922);
  - USD(I&S) connection to cleared defense contractors (~12,000);
  - USD(A&S)/Industrial Policy's ongoing engagements with defense industry associations;
  - NSA's engagement with DIB and other companies; and
  - Policy's PPD-21 connection to the ND-ISAC and SCC (~300).

16 Critical Infrastructure Sectors and Corresponding Sector Risk Management Agencies (SRMA)



FINANCIAL	Treasury	CHEMICAL	DHS (CISA)
FOOD & AGRICULTURE	USDA & HHS	COMMERCIAL FACILITIES	DHS (CISA)
GOVERNMENT FACILITIES	GSA & DHS (FPS)	COMMUNICATIONS	DHS (CISA)
HEALTHCARE & PUBLIC HEALTH	HHS	CRITICAL MANUFACTURING	DHS (CISA)
INFORMATION TECHNOLOGY	DHS (CISA)	DAMS	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)	DEFENSE INDUSTRIAL BASE	★ DOD
TRANSPORTATIONS SYSTEMS	(TSA & USCG)	EMERGENCY SERVICES	DHS (CISA)
WATER	EPA	ENERGY	DOE



NSA CCC

- Who Are We?
  - NSA's Cybersecurity Collaboration Center harnesses the power of industry partnerships to prevent and eradicate foreign cyber threats from our nation's most critical networks
  - Our efforts focus on the DoD, the DIB, and National Security Systems (NSS)

- NSA's DIB Cybersecurity Initiatives
  - NSA has partnered with DoD to **expand its information sharing capabilities** with the DIB. We leverage our foreign intelligence insights & technical expertise to **better protect critical DoD information** residing on DIB information systems and networks.
  - Efforts Include:
    - ➢ Bi-directional sharing of cybersecurity information
    - ➢ Jointly develop tradecraft for identifying malicious cyber actors
    - ➢ Develop, share, and amplify tailored mitigation guidance to the DIB
    - ➢ Provide direct cybersecurity assistance to identify, mitigate, and thwart threats to their networks

NSA CCC (Cont.)

To better protect DoD information on DIB networks, NSA offers the following no-cost cybersecurity services to DIB companies with an active DoD contract and access to controlled DoD information

Protect DNS/Secure Web Gateway

- Scalable GovShield serviced from Akamai
- Offers real-time DNS malicious query introduction
- Integrates Akamai's commercial threat intelligence with NSA analytics and IOCS

Vulnerability Scanning and Mitigation

- Leverage commercial and open-source information to expose vulnerabilities
- Automated aggregation and reporting to companies
- Identify probable exploitation routes and engage before compromise

Threat Intelligence Collaboration

- Tailored distribution of NSA cybersecurity products
- Timely and prioritized sharing of IOCs and mitigations
- Collaboration with NSA analysts on findings

DC3/DCISE

- Trusted partnership with 900+ DIB Companies
    - Bi-directional cyber threat information sharing (products/submission available via DIBNet)
        - Products range from IOC-based to long form narrative risk management reports (both Secret and Unclassified) to meet varied needs
        - No-cost malware and forensic analyses (Electronic Malware Submission Portal)
        - DIB Vulnerability Disclosure Program Pilot
    - Engagement opportunities (ranging from intimate to broad; transition to virtual- expanding capability)
        - A2A/B2B
        - Webconferences
        - RPEX/VIPEX
        - TechEx (DIB CS Working Group meetings; POWG and TAWG)
    - Cybersecurity as a Service Offerings
        - Emulation
        - MISCyber Resilience Analysis (CRA)
        - DCISE^3
        - Krystal Ball
        - Adversary P and Automated Indicator Sharing
- DoD-designated focal point to receive all mandated cyber incident reporting involving defense contractor unclassified networks

Questions & Answers

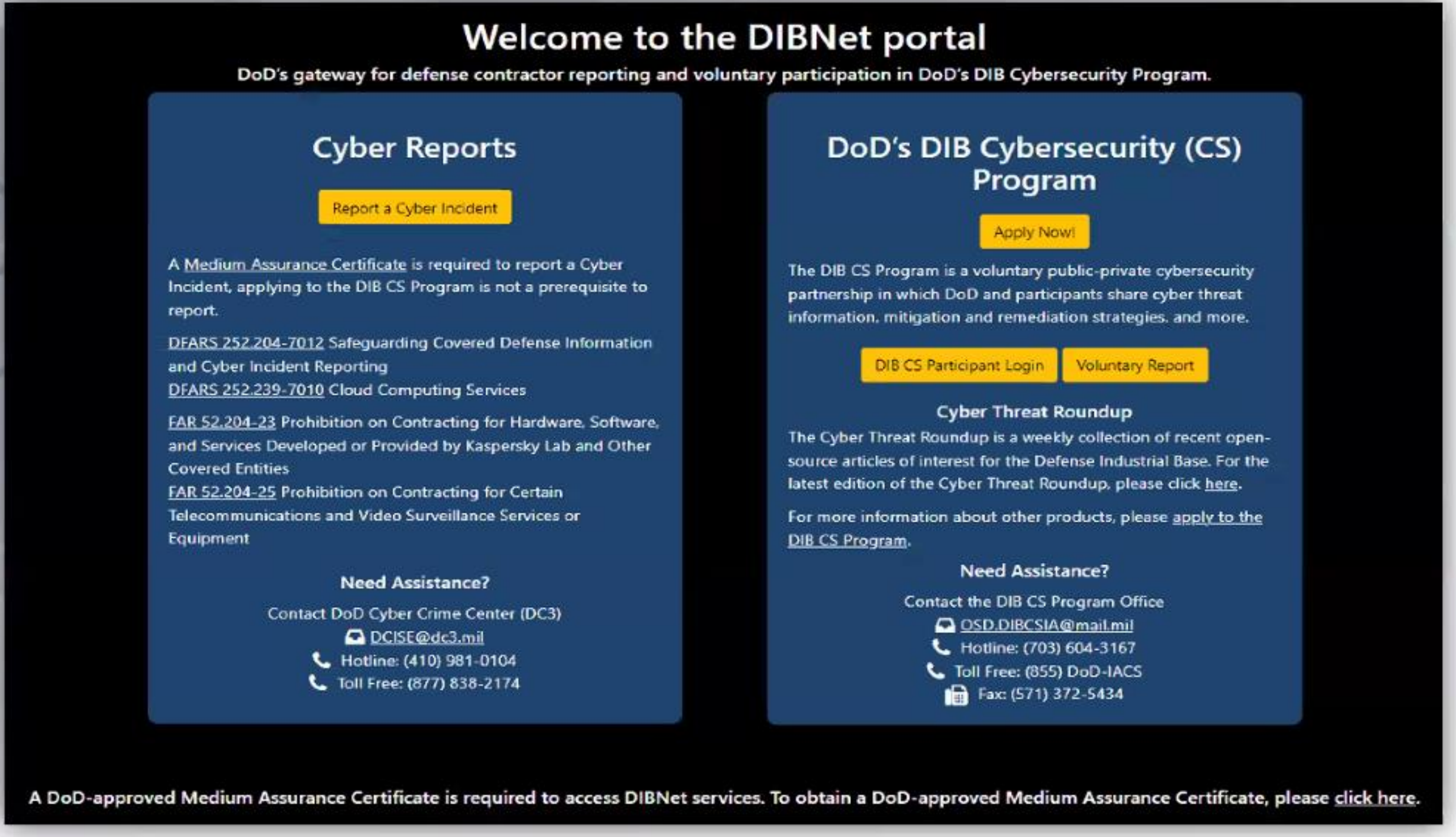
Contact Us

DoD's DIB CS Program
OSD.DIBCSIA@mail.mil

DC3/DCISE
DC3.DCISE@us.af.mil

NSA's CCC
DIB_Defense@cyber.nsa.gov

For more information, visit DIBNet at https://dibnet.dod.mil



Welcome to the DIBNet portal

DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?

Contact DoD Cyber Crime Center (DC3)
✉ DCISE@dc3.mil
☎ Hotline: (410) 981-0104
☎ Toll Free: (877) 838-2174

DoD's DIB Cybersecurity (CS) Program

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

Cyber Threat Roundup

The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

For more information about other products, please apply to the DIB CS Program.

Need Assistance?

Contact the DIB CS Program Office
✉ OSD.DIBCSIA@mail.mil
☎ Hotline: (703) 604-3167
☎ Toll Free: (855) DoD-IACS
📠 Fax: (571) 372-5434

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please click here.

Speakers

- Kevin DeLaney
- Dave McKeown, DoD CISO
- Kristi Hunt, USD(P) = Under Secretary of Defense for Policy
- Kristina Walter, NSA CCC
- Krystal Covey, DC3