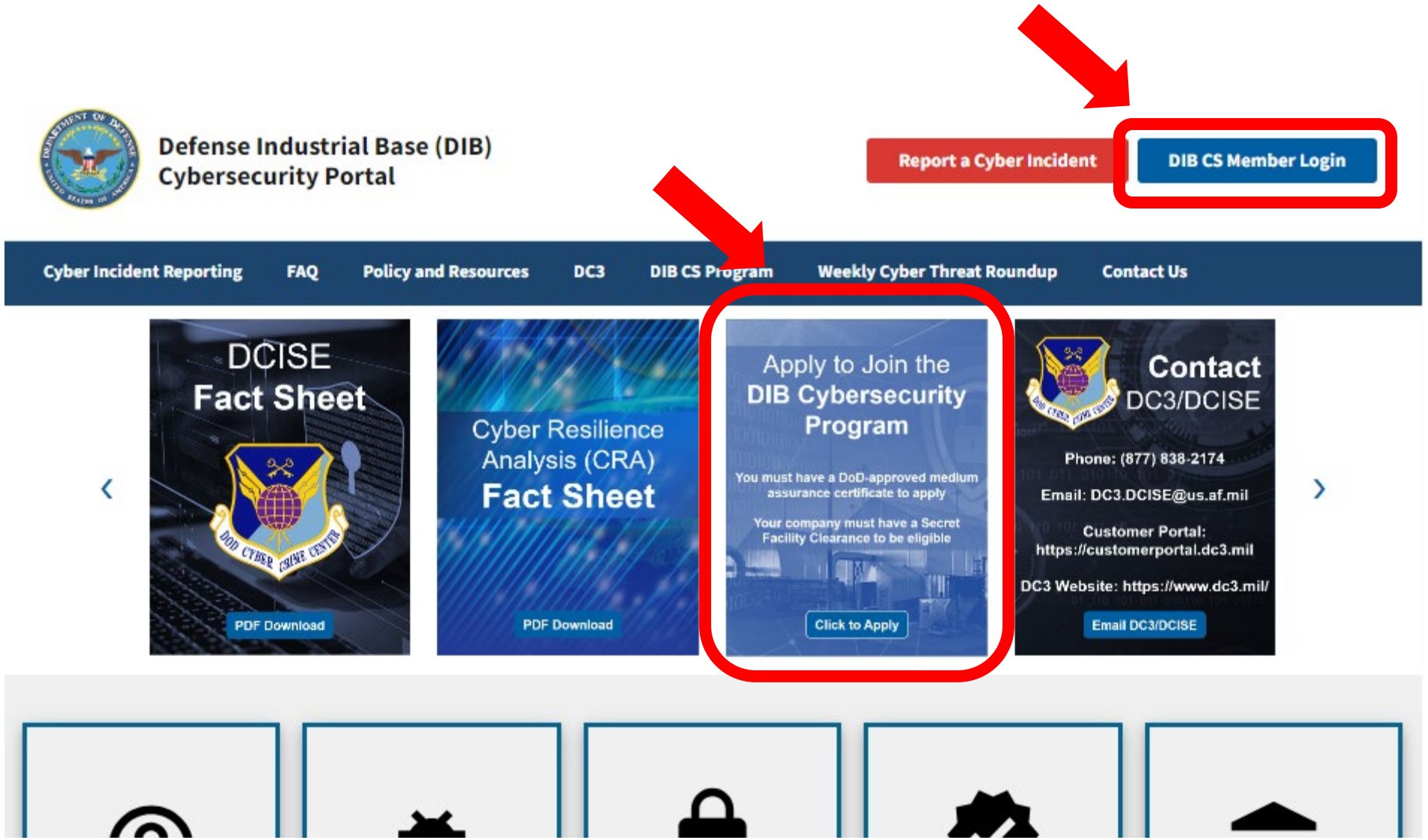

Defense Industrial Base (DIB)
Cybersecurity Portal
Report a Cyber Incident
DIB CS Member Login
Cyber Incident Reporting
FAQ
Policy and Resources
DC3
DIB CS Program
Weekly Cyber Threat Roundup
Contact Us
DCISE
Fact Sheet
PDF Download
Cyber Resilience
Analysis (CRA)
Fact Sheet
PDF Download
Apply to Join the
DIB Cybersecurity
Program
You must have a DoD-approved medium assurance certificate to apply
Your company must have a Secret Facility Clearance to be eligible
Click to Apply
Contact
DC3/DCISE
Phone: (877) 838-2174
Email: DC3.DCISE@us.af.mil
Customer Portal:
https://customerportal.dc3.mil
DC3 Website: https://www.dc3.mil/
Email DC3/DCISE

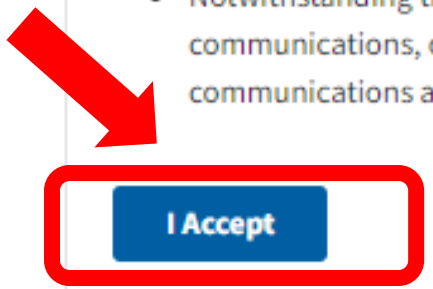
DIBNet

DoD Information System Standard Notice and Consent

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.



I Accept

DIBNet

Privacy Statement

Authorities: 10 U.S.C. 391, "Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors and Certain Other Contractors;" 10 U.S.C. 393, "Reporting on Penetrations of Networks and Information Systems of Certain Contractors;" 10 U.S.C. 2224, "Defense Information Assurance Program;" 50 U.S.C. 3330, "Reports to the Intelligence Community on Penetrations of Networks and Information Systems of Certain Contractors;" 32 Code of Federal Regulations (CFR) part 236, "Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities;" and DoDI 5205.13, "Defense Industrial Base (DIB) Cybersecurity (CS) Activities."

Purpose: Administrative management of the DIB CS Program's information sharing activities. Personal information is covered by OSD SORN DCIO 01, Defense Industrial Base (DIB) Cybersecurity/Information Assurance Records, available at: https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.pdf

Routine Use(s): In addition to the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- DIB company point of contact information may be provided to other participating DIB companies to facilitate the sharing of information and expertise related to the DIB CS Program including cyber threat information and best practices, and mitigation strategies.
- Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.
- Counterintelligence Purpose Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.
- Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense/Joint Staff compilation of systems of records notices may apply to this system. The complete list of the DoD blanket routine uses can be found online at: https://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Any release of information contained in this system of records outside the DoD will be compatible with the purpose(s) for which the information is collected and maintained.

Disclosure: Voluntary. However, failure to provide requested information may limit the ability of the DoD to contact the individual or provide other information necessary to facilitate this program.

Privacy Impact Assessment (PIA). The PIA addresses the processes in place to protect information provided by DoD contractors reporting cyber incidents. The PIA for the Defense Industrial Base (DIB) Cybersecurity Activities is available at: https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA_Section1.pdf

Freedom of Information Act (FOIA). Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 C.F.R. Parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

Agency Disclosure Notic
OMB CONTROL NUMB -0490
OMB EXPIRATION /31/2025
The public re urden for this collection of information, 0704-0490, is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

I Accept

DIBNet

Company Application

1 Company — 2 Company Representative — 3 CEO — 4 CIO — 5 CISO — 6 Additional POC — 7 Summary

1 of 7 Company

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

Company Information

Field is required

Company Name *

UEI

Field is required

CAGE Code *

NAICS

Company Security Level Description

Company Size

I certify that my company handles (e.g. processes, stores, develops, or transits) DoD Controlled Unclassified Information (CUI).

☑ Certify*

Company Location and Contact Information

Field is required

Street address line 1 *

Street address line 2 (Optional)

Field is required

City *

Field is required

State *

Invalid zip code

123

Field is required

Phone *

Continue ›

Cancel

DIBNet

Company Application

1 Company — 2 Company Representative — 3 CEO — 4 CIO — 5 CISO — 6 Additional POC — 7 Summary

2 of 7 Company Representative

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

Are you the Company Representative? *

- (●) Yes
- ( ) No

The Company Representative is the individual authorized to act on behalf of the company during the application process to the DIB CS Program. If your company is eligible for the DIB CS Program the Company Representative is responsible for updating authorized POC's with the Program. The DIB CS Program hosts quarterly working group meetings with industry participants and Government stakeholders to discuss relevant cyber policies and technologies. The Company Representative will receive an invitation to these meetings.

Company Representative Information

Firstname | MI | Lastname

Title

Work Contact Information

☐ Same as Company Address

Street address line 1

Street address line 2 (Optional)

City | State

Zip Code | Work Phone

Email Address *

‹ Back | Continue › | Save And Quit | Cancel

DIBNet

Company Application

1 Company — 2 Company Representative — 3 CEO — 4 CIO — 5 CISO — 6 Additional POC — 7 Summary

3 of 7 CEO

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

CEO (or equivalent) Information

☐ Same as Company Representative

First Name * | MI | Last Name *

Title

Work Phone

Email Address *

‹ Back | Continue › | Save And Quit | Cancel

DIBNet

Company Application

1 Company — 2 Company Representative — 3 CEO — 4 CIO — 5 CISO — 6 Additional POC — 7 Summary

4 of 7 CIO

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

CIO (or equivalent) Information

The DIB CS Program hosts quarterly working group meetings with industry participants and Government stakeholders to discuss relevant cyber policies and technologies. The CIO will receive an invitation to these meetings.

☐ Same as Company Representative

First Name * | MI | Last Name *

Title

Work Phone

Email Address *

‹ Back | Continue › | Save And Quit | Cancel

DIBNet

Company Application

1 Company — 2 Company Representative — 3 CEO — 4 CIO — 5 CISO — 6 Additional POC — 7 Summary

5 of 7 CISO

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

Chief Information Security Officer (CISO) (or equivalent) Information

The DIB CS Program hosts quarterly working group meetings with industry participants and Government stakeholders to discuss relevant cyber policies and technologies. The CISO will receive an invitation to these meetings.

☐ Same as Company Representative

First Name * | MI | Last Name *

Title

Work Phone

Email Address *

‹ Back | Continue › | Save And Quit | Cancel

DIBNet

Company Application

1 Company | 2 Company Representative | 3 CEO | 4 CIO | 5 CISO | 6 Additional POC | 7 Summary

6 of 7 Additional POC

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

Chief Security Officer (CSO)/Facility Security Officer (FSO)

First Name | MI | Last Name

Title

Email Address

Technical Personnel

A Technical Personnel is a company employee that is in, or will be in possession of their own DoD-approved medium assurance certificate, will receive automated Participant Reports through the DIBNet Portal, will be invited to attend DIB CS Program Working Groups

☐ Same as Company Representative

Technical Personnel Remove

First Name | MI | Last Name

Title

Email Address

+ Add Additional Technical Personnel

USG Point of Contact

This information may be made available to other DIBNet Users from your Company when submitting a cyber incident report at a future date. Any USG POC added here now will not be contacted at this time.

+ Add Additional USG Point of Contact

‹ Back | Continue › | Save And Quit | Cancel

This information may be made available to other DIBNet Users from your Company when submitting a cyber incident report at a future date. Any USG POC added here now will not be contacted at this time.

USG Point of Contact Remove

First Name | Last Name

Title

Address

City | -- State --

Postal Code | -- Country --

Telephone

Email Address

-- Time Zone --

Contract Number(s)

-- Contract or Other Agreement Clearance Level --

-- Are you the primary Contractor? --

+ Add Additional USG Point of Contact

‹ Back | Continue › | Save And Quit | Cancel

DIBNet

Company Application

1 Company | 2 Company Representative | 3 CEO | 4 CIO | 5 CISO | 6 Additional POC | 7 Summary

7 of 7 Summary

Please provide information about your organization and points of contact (POCs) below. Please review the summary page and check "Certify Application" before attempting to submit. Once your application has been submitted, DoD will verify data with the listed Chief/Facility Security Officer (CSO/FSO), if applicable. The FSO for the CAGE code should match what appears in Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS).
* indicates a required field.

Print Summary

Company Information Edit

Company Name:

Test Company Name

UEI:	CAGE Code:	NAICS:
123456789101	**12345**	

Company Security Level Description:

Government Secret

Company Size:

Small 251-1,000

Company Representative Information Edit

First Name:	M.I:	Last Name:
Company	**A**	**Representative**

Title:

CEO

Street 1:

123 Company Street

Street 2:

Suite 123

I certify that my company handles (e.g. processes, stores, develops, or transits) DoD Controlled Unclassified Information (CUI):

Certify

Street 1:

123 Company Street

Street 2:

Suite 123

City:	State:	Zip Code:
Springfield	**Alaska**	**12345**

Phone:

111-222-3333

City:	State:	Zip Code:
Springfield	**Alaska**	**12345**

Work Phone:

111-222-3333

Email Address:

company-rep@testcompanyname.biz

CEO Information Edit

First Name:	M.I:	Last Name:
Company	**A**	**Representative**

Title:

CEO

Work Phone:

111-222-3333

Email Address:

company-rep@testcompanyname.biz

CIO Information Edit

First Name:	M.I:	Last Name:
Company	**A**	**Representative**

Title:

CEO

Work Phone:

111-222-3333

Email Address:

company-rep@testcompanyname.biz

CISO Information Edit

First Name:	M.I:	Last Name:
Company	**A**	**Representative**

Title:

CEO

Work Phone:

111-222-3333

Email Address:

company-rep@testcompanyname.biz

Additional POCs

Chief Security Officer Information Edit

First Name: **Security**

M.I: **A**

Last Name: **Officer**

Title: **FSO**

Email Address: **security-officer@testcompanyname.biz**

Technical Personnel #1 Information

Edit

First Name: **Company**

M.I: **A**

Last Name: **Representative**

Title: **CEO**

Email Address: **company-rep@testcompanyname.biz**

USG Personnel #1 Information Edit

First Name: **John**

Last Name: **Doe**

Title: **COR/KO**

Address: **1234 Government Blvd**

City: **Washington**

State: **District of Columbia**

Country:

United States of America

Postal Code:

12345

Telephone:

111-222-3333

Email Address:

john-doe@mail.mil.biz

Time Zone:

(GMT-2:00) Mid-Atlantic

Contract Numbers:

123456789101, 09876543211

Contract or Other Agreement Clearance Level:

Secret

Are you the primary contractor?

Yes

I certify that the information provided is accurate to the best of my knowledge. I understand that DoD will confirm the accuracy of the information with my company and other components in the DoD.

Certify Application *

‹ Back | Submit | Save And Quit | Cancel