

Welcome to the DIBNet portal

DoD's gateway for defense contractor cyber incident reporting and voluntary participation in DoD's Cybersecurity Program

Report a Cyber Incident

[Report](#)

A DoD-approved Medium Assurance Certificate is required to access the reporting module. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).

Do you know what to report? [See below](#).

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 cyber threat information sharing program established by DoD to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems.

To apply to the DIB CS Program, a DoD-approved Medium Assurance Certificate is required. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).

[Apply Now!](#)

Need assistance?

Contact the DIB CS Program Office

OSD.DIBCSIA@mail.mil

(703) 604-3167

Toll Free: (855) DoD-IACS

Fax: (571) 372-5434

Reporting a Cyber Incident

[For DoD Contractors](#)

About the DIB CS Program

[What is the DoD's DIB CS program?](#)

https://dibnet.dod.mil/portal/intranet/

The screenshot shows a web portal for reporting a cyber incident. A modal dialog box titled "Select a certificate" is open, displaying a table of certificates. The table has columns for Subject, Issuer, and Serial. One certificate is listed: Subject: DoD CIO.Mailbox DIB CS IA.Progra..., Issuer: DOD ID SW CA-38, Serial: 028EAB. Below the table are buttons for "Certificate information", "OK", and "Cancel".

Subject	Issuer	Serial
DoD CIO.Mailbox DIB CS IA.Progra...	DOD ID SW CA-38	028EAB

Background text on the page includes:

- Report**: DoD's gateway for reporting a cyber incident. A DoD-approved Medium Assurance Certificate is required to access the reporting module. Do you know what to report? See below.
- Need assistance?**: Contact DoD Cyber Crime Center (DC3). Email: DCISE@dc3.mil. Hotline: (410) 981-0104. Toll Free: (877) 838-2174.
- Security (CS)**: To apply to the DIB CS Program, a DoD-approved Medium Assurance Certificate is required. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).
- Need assistance?**: Contact the DIB CS Program Office. Email: OSD.DIBCSIA@mail.mil. (703) 604-3167. Toll Free: (855) DoD-IACS. Fax: (571) 372-5434.

Reporting a Cyber Incident


For DoD Contractors

About the DIB CS Program

What is the DoD's DIB CS program?

← → C https://dibnet.dod.mil/portal/intranet/USG

UNCLASSIFIED//FOUO



Defense Industrial Base (DIB) Cybersecurity (CS)
Information Sharing Program

0704-0490
XXXXXXXX

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.

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 DoD 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CSIA) 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) Cyber Security/Information Assurance Records, available at: <http://www.gpo.gov/foi/syplg/FR-2015-05-21/pdf/2015-12324.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: <http://dpcdd.defense.gov/Privacy/SORNIndex/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: http://dodcio.defense.gov/Portals/0/Documents/PIA_DIB%20CS%20program_Aug%202015_corrected.pdf?ver=2016-09-22-113831

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 Notice:

OMB CONTROL NUMBER: 0704-0490

OMB EXPIRATION DATE: 11/30/2019

The public reporting burden for this collection of information 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 this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, 6000 Defense Pentagon ATTN: DIB CS Program, Washington, DC 20301-6000 (0704-0490). 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 Agree

Company Application Process

Welcome to the Defense Industrial Base (DIB) Cyber Security (CS) Program

Company Application Form

Please provide information about your organization and points of contact (POCs) below. Fields marked an * are required. 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 Chief Facility Security Officer (CSO/FSO).
* =Required Field

Company Company Representative CEO CIO CISO Additional POC Summary

Company Information

Company Name * :

CAGE Code * :

Company Location and Contact Information

Street 1 * :

Street 2 :

City * :

State * :

Zip Code * :

Fax :

Phone * :

Additional Company Information

Additional Information :

Save

Next

Review and Certify

Company Application Process

Welcome to the Defense Industrial Base (DIB) Cyber Security (CS) Program

Company Application Form

Please provide information about your organization and points of contact (POCs) below. Fields marked with an * are required. 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 Chief/Facility Security Officer (CSO/FSO).
* =Required Field

- Company
- Company Representative
- CEO
- CIO
- CISO
- Additional POC
- Summary

Company Representative Information

First Name * :

Middle Initial :

Last Name * :

Title * :

US Citizen :

Clearance :

Work Contact Information

Street 1 * :

Street 2 :

City * :

State * :

Zip Code * :

Work Phone * :

Fax :

Email Address * :

Save | Res | Review and Certifi

Company Application Process

Welcome to the Defense Industrial Base (DIB) Cyber Security (CS) Program

Company Application Form

Please provide information about your organization and points of contact (POCs) below. Fields marked an * are required. 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 Chief/Facility Security Officer (CSO/FSO).
* = Required Field

Company Company Representative **CEO** CIO CISO Additional POC Summary

Same as Company Representative

CEO (or equivalent) Information

First Name * :
Middle Initial :
Last Name * :
Title * :

Work Contact Information

Work Phone :
Email Address * :

Executive Assistant (EA) Work Contact Information

EA First Name :
EA Middle Initial :
EA Last Name :
EA Phone :
EA Email :

C

Save

Company Company Representative CEO CIO CISO Additional POC Summary

Same as Company Representative

CIO (or equivalent) Information

First Name * :
Middle Initial :
Last Name * :
Title * :

Work Contact Information

Street 1 :
Street 2 :
City :
State :
Zip Code :
Phone :
Email Address * :

Executive Assistant (EA) Work Contact Information

EA First Name :
EA Middle Initial :
EA Last Name :
EA Phone :
EA Email :

Save Rese Review and Certifi

Same as Company Representative

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

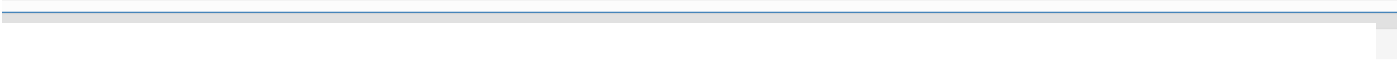
First Name * :
Middle Initial :
Last Name * :
Title * :

Work Contact Information

Street 1 :
Street 2 :
City :
State :
Zip Code :
Phone :
Email Address * :

Executive Assistant (EA) Work Contact Information

EA First Name :
EA Middle Initial :
EA Last Name :
EA Phone :
EA Email :



0704-0490
XXXXXXXX

Company Company Representative CEO CIO CISO Additional POC Summary

Chief Privacy Officer (or equivalent)

First Name * :
Middle Initial :
Last Name * :
Title * :
Work Email * :
Not Applicable

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

First Name * :
Middle Initial :
Last Name * :
Title * :
Work Email * :

General Counsel Representative

First Name * :
Middle Initial :
Last Name * :
Title * :
Work Email * :

Additional POCs

Administrative Personnel

First Name :
Middle Initial :
Last Name :
Title :
Work Email :
US Citizen :
Clearance :

Policy Personnel

First Name :
Middle Initial :
Last Name :
Title :
Work Email :
US Citizen :
Clearance :

Authorized Incident Report Submitter

First Name :
Middle Initial :
Last Name :
Title :
Work Email :
US Citizen :
Clearance :

Technical Personnel

First Name :
Middle Initial :
Last Name :
Title :
Work Email :
US Citizen :
Clearance :

Additional POCs (up to 10)
*Add Additional POC

Save Review and Certify

Summary

Print Summary

Application Status: Application not yet saved

Company Information [\[Edit\]](#)

Company Name	CAGE Code
Street 1	Fax
Street 2	Zip Code
City	
State	
Phone	

Additional Information

Company Representative Information [\[Edit\]](#)

First Name	Last Name
Middle Initial	Title
US Citizen	Work Phone
Clearance	Fax
Work Email Address	

CEO Information [\[Edit\]](#)

First Name	Last Name
Middle Initial	Title
Work Phone	EA First Name
Work Email Address	EA Middle Initial
EA Last Name	EA Email
EA Phone	

CIO Information [\[Edit\]](#)

First Name	Last Name
Middle Initial	Title
Street 1	Work City
Street 2	Work State
Work Zip Code	Work Email Address
Work Phone	EA First Name

EA Middle Initial

EA Phone

EA Last Name

EA Email

Additional POC Information

Chief Privacy Officer Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Chief Security Officer Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

General Counsel Representative Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Administrative Personnel Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Clearance

US Citizen

Policy Personnel Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Clearance

US Citizen

Authorized Incident Report Submitter Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Clearance

US Citizen

Technical Personnel Information [\[Edit\]](#)

First Name

Last Name

Middle Initial

Title

Work Email

Clearance

US Citizen

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, including with my company and the Defense Security S

Certify Application

[Print Summary](#)

[Submit Application](#)

[Save](#)

[Reset](#)