



CISA ALERT

Due to increasing geopolitical tensions, the Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) has issued a "Shields Up" advisory (www.cisa.gov/shields-up). This is relevant to all DIB Companies.



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](#)

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](#)

DC3 Weekly Cyber Threat Roundup

[PDF Download](#)

DC3 Fact Sheet

[PDF Download](#)

DoD Information System Notice and Consent Page

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

Privacy Policy

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) Cyber Security/Information Assurance Records, available at: <https://dpcl.d.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: <http://dpcl.d.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.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 Notice:

OMB CONTROL NUMBER: 0704-0490

OMB EXPIRATION DATE: 11/30/2022

The public reporting burden 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 burden 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.

Company Information

Example Company X | 🗑️

Field is required

DUNS * | ▼

Field is required

CAGE Code * | ▼

NAICS | ▼

Company Size | ▼

Company Location and Contact Information

45 BROADWAY FL 25

Street address line 2 (Optional)

NEW YORK New York X | ▼

10006

122222222222222222 Fax

2 of 7 **Company Representative**

Company Representative Information

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.

TEST [icon] Z TEst

test

Work Contact Information

123 st

Street address line 2 (Optional)

Arlington Arizona [X] [v]

20121

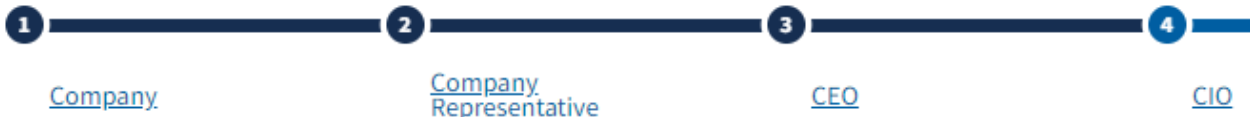


3 of 7 CEO

CEO (or equivalent) Information

Same as Company Representative

TEST	M	TEst
------	---	------



4 of 7 CIO

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

[< Back](#)[Continue >](#)[Save](#)[Cancel](#)



5 of 7 CISO

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

TEST M TEst

test

123213232323

testcert1@mail.dibnetu.mil

< Back

Continue >

Save

Cancel

6 of 7 **Additional POC****Chief Security Officer (CSO)/Facility Security Officer (FSO)**

test	<input type="checkbox"/>	M	test
------	--------------------------	---	------

Technical Personnel

- i** 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 DIB CS Program Working Groups
* indicates a required field.

 Same as Company Representative
Technical Personnel[Remove](#)

TEST	<input type="checkbox"/>	M	TEst
------	--------------------------	---	------

1

[Company](#)

2

[Company Representative](#)

3

[CEO](#)

4

[CIO](#)

5

[CISO](#)

6

[Additional POC](#)

7

[Summary](#)

7

of 7 **Summary** Print Summary

Company Information

[Edit](#)

Company Name:

Example Company

Company Status:

REGISTERED

Framework Agreement Signed Date:

06/22/2022

DUNS:

Missing Field

CAGE Code:

Missing Field

NAICS:

Company Size:

Street 1:

45 BROADWAY FL 25

Street 2:

City:

NEW YORK

State:

New York

Zip Code:

10006

Phone:

122222222222

Fax:

Company Representative Information

[Edit](#)

First Name:

TEST

M.I.:

Z

Last Name:

TEst

Title:

test

Street 1:

123 st

Street 2:

City:

Arlington

State:

Arizona

Zip Code:

20121

Work Phone:

123213232323

Fax:

Email Address: