



# 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](#)



**DC3 Weekly  
Cyber Threat  
Roundup**

[PDF Download](#)

**DC3  
Fact Sheet**

[PDF Download](#)

**DCISE  
Fact Sheet**

[PDF Download](#)

**Cyber Resilience  
Analysis (CRA)  
Fact Sheet**

[PDF Download](#)



**FAQ and Factsheets**

[More Info](#)



**Submit Malware**

[More Info](#)



**DoD Cyber Crime  
Center (DC3)**

[More Info](#)



**Obtain a Medium  
Assurance Certificate**

[More Info](#)



**Policy and Resources**

[More Info](#)

CUI



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

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.



Please click [here](#) if you have any feedback on this form

[About ICF](#)



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

**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://www.gpo.gov/fdsys/pkg/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:

- **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://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\\_Section1.pdf](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 Notice:**

OMB CONTROL NUMBER: 0704-0489

OMB EXPIRATION DATE: 12/31/2024

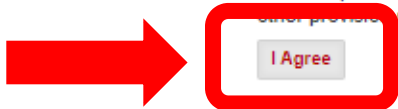
OMB CONTROL NUMBER: 0704-0478

OMB EXPIRATION DATE: 10/31/2025

The public reporting burden for this collection of information, 0704-0489, is estimated to average 2 hours 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](mailto: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.

Please [CLICK here](#) if you have any feedback on this form

[About ICF](#)





The Incident Collection Format (ICF) is used by DoD contactors to report cyber threat information. Reporting requirements are outlined in [DFARS 252.204-7012](#), [DFARS 252.239-7010](#), [FAR 52.204-23](#) and [FAR 52.204-25](#). If you need to start a new cyber incident report in response to contractually-mandated requirements, click on “Start a New Incident Report” and you will be asked a series of questions to determine the appropriate report type (Mandatory Report, Cloud Service Provider Report, Prohibited Item Report). If you are an active member in the voluntary [DIB Cybersecurity Program](#) and would like to submit a voluntary report, please [click here](#) to bypass the wizard used for contractually-mandated report types. If you are unsure if your report is mandatory or voluntary, please use the wizard at “Start a New Incident Report.”

## New Report



[Start a New Incident Report](#)

## Saved Reports

Saved reports are retained for 72 hours. After 72 hours saved reports are deleted.

[Update an In-Progress Incident Report](#)

## Past Reports

Submitted reports are available for 90 days to facilitate submission of follow-on reports. After 90 days, only the Incident Number remains available for reference. Malware submissions should be made on the [Malware Portal](#).

[Submit a Follow-on Report](#)

### Routine Uses

**Voluntary DIB Cybersecurity Activities Use:** Share cybersecurity threat information and best practices to enhance and supplement DIB participants' capabilities to safeguard DoD unclassified information that resides on, or transits DIB unclassified information systems.

**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.

Please click [here](#) if you have any feedback on this form

[About ICF](#)



### ICF User Instructions

This wizard will assist in determining which report type to submit. Reporting requirements are outlined in [DFARS 252.204-7012](#) (Mandatory Report), [DFARS 252.239-7010](#) (Cloud Service Provider Report), [FAR 52.204-23](#) and [FAR 52.204-25](#) (Prohibited Item Report). Each question will align your report with a contractual requirement. If you are a member of the voluntary [DIB CS Program](#) and would like to submit a voluntary report, please [click here](#) to bypass the wizard for contractually-mandated report types. If you need to submit a follow-on report, please [go back](#) and click on "Submit Follow-On Report" from your [Past Reports](#).

Does this incident affect, or possibly affect, the contractor's ability to perform the requirements of a contract that is designated as operationally critical support? ([DFARS 252.204-7012](#))

Does this incident affect, or possibly affect, Covered Defense Information? ([DFARS 252.204-7012](#))

You have indicated that the incident being submitted does NOT meet the requirements for mandated reporting under [DFARS 252.204-7012](#). If you have questions, please contact DoD Cyber Crime Center (DC3) at [DC3.DCISE@us.af.mil](mailto:DC3.DCISE@us.af.mil), or (410) 981-0104.

Does this incident identify Prohibited Hardware, Software, or Services provided used by the Government during contract performance? ([FAR 52.204-23](#) and [FAR 52.204-25](#))

Does this incident relate to a Cloud Computing Service Provider, when used to provide information technology services to process data on behalf of the DOD in the performance of the contract? ([DFARS 252.239-7010](#))

Does this incident relate to a covered article under the Federal Acquisition Security Council Supply Chain Security Act that was discovered during the performance of the contract? ([FAR 52.204-30](#))



## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

General  
Information

I. Company  
Information

II. Company  
POC  
Information

III. Incident  
Information

Supplemental  
Incident  
Information

IV. Ancillary  
Information

Preview

This Incident Collection Format (ICF) is used by DoD contractors to submit voluntary cyber threat information to the DC3/DCISE.

Contractors should use this format to share cyber threat information that is of interest for cyber situational awareness as well as cyber threat indicators that may be valuable in alerting others to better counter threat actor activity.

The information will be shared on a non-attribution basis. Attribution information uniquely identifies the respondent or respondent's unique business activities, whether directly or indirectly, to include the grouping of data elements that directly point to the respondent (e.g., company facility location, company proprietary information, etc). DC3/DCISE will use the information to prepare analytic products or response actions that does not assign attribution to the originator, e.g., information regarding threats, vulnerabilities, best practices, etc.

Non attribution products developed by DC3/DCISE will be disseminated to Federal Government Agencies and participants in the voluntary DoD's DIB cybersecurity information sharing program.

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 establish 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.

### General Information Collection

\* Are you a participant in the DIB CS Program?

Yes

No

Is this an Indicator Only submission?

Yes

No

Cancel

Save and Exit

Next





## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

[General Information](#)[I. Company Information](#)[II. Company POC Information](#)[III. Incident Information](#)[Supplemental Incident Information](#)[IV. Ancillary Information](#)[Preview](#)

### Company Information

Please provide identifying information for the company submitting the incident. Company information is suggested using data from SAM.gov

\* Company Name

\* Address

\* City

\* State

\* Country

\* Postal Code

[Previous](#)[Cancel](#)[Save and Exit](#)[Next](#)

Please click [here](#) if you have any feedback on this form

[About ICF](#)



## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

General Information | I. Company Information | **II. Company POC Information** | III. Incident Information | Supplemental Incident Information | IV. Ancillary Information | Preview

### Company Point of Contact Information

You may enter multiple points of contact using the 'Add POC' button below.

#### Point of Contact Information (POC 1)

Saved POCs:

* Last Name	* First Name
<input type="text"/>	<input type="text"/>
* Position/Title	* Work Telephone
<input type="text"/>	<input type="text"/>
* Email Address	* Time Zone
<input type="text"/>	Choose <input type="text"/>

←





## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

[General Information](#)[I. Company Information](#)[II. Company POC Information](#)[III. Incident Information](#)[Supplemental Incident Information](#)[IV. Ancillary Information](#)[Preview](#)

### Incident Information

Date Incident Occurred

Date/Time

Time Zone

(GMT-5:00) Eastern Time (US & Canada), Bogota, Lima



[Clear Incident Date Occurred](#)

Date Incident Discovered

Date/Time

Time Zone

(GMT-5:00) Eastern Time (US & Canada), Bogota, Lima



[Clear Incident Date Discovered](#)

Location(s) of Compromise

\* Incident Location CAGE Code(s)

Detection Method

Choose



\* Type of Incident

- Unknown
- Unauthorized or Inadvertent Release
- Unauthorized Access
- Spillage/Improper Handling
- Lost Device
- Stolen Device
- Insider Threat
- PII Exposure
- Data Exfiltration
- Other

Incident Outcome

Choose ▼

Incident Mitigation Date

Date/Time


Time Zone

(GMT-5:00) Eastern Time (US & Canada), Bogota, Lima ▼

**Clear Incident Mitigation Date**

\* Incident Narrative (Chronological explanation of incident, threat actor TTPs, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred). For DIB CS Program participants, the information included in this field will be shared in the Participant report. Please do not include attributional or sensitive information.

[?]

**Previous** **Cancel** **Save and Exit** **Next** 



### Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

- General Information
- I. Company Information
- II. Company POC Information
- III. Incident Information
- Supplemental Incident Information
- IV. Ancillary Information
- Preview

### Supplemental Incident Information

Was U.S. Government or Military PII compromised or potentially compromised in the cyber incident?

Yes  
 No  
 Unknown

Known Advanced Persistent Threat (APT) Involved

Yes  
 No  
 Unknown

Incident Detected by DC3/DCISE Indicator?

Yes  
 No

Any additional information relevant to the incident not included above (Note: This response may contain attributional or sensitive information. It is for DC3/DCISE use only.):

\* Has this information been shared with any other Federal Government agency?

Yes  
 No

Enter any other tracking numbers and the associated point of contact (if applicable)

- Previous
  - Cancel
  - Save and Exit
  - Next
-



## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

[General Information](#)[I. Company Information](#)[II. Company POC Information](#)[III. Incident Information](#)[Supplemental Incident Information](#)[IV. Ancillary Information](#)[Preview](#)

### Ancillary Information

\* Does this report include known or potentially sensitive Personally Identifiable Information (PII)?

- Yes  
 No

\* Do you authorize DC3 to provide this report with attribution to DCSA?

- Yes  
 No

\* Do you have malicious software related to the cyber incident ready for submission to DC3/DCISE?

*Malware may be submitted using the Malware portal (link to: <https://ems.dc3on.gov/>) - link will open in a new tab*

- Yes  
 No

[Previous](#)[Cancel](#)[Save and Exit](#)[Next](#)



## Voluntary Cyber Threat Information Sharing/Indicator Only Report

Questions marked with \* are required

[General Information](#)[I. Company Information](#)[II. Company POC Information](#)[III. Incident Information](#)[Supplemental Incident Information](#)[IV. Ancillary Information](#)[Preview](#)

**ATTENTION:** You must click the "Submit" button at the bottom of this page in order to complete the submission of this form.

### General Information Collection

[Edit](#)

Are you a participant in the DIB CS Program? Yes  
Is this an Indicator Only submission? No  
Is this a follow-on report? No

### Company Information

[Edit](#)

Company Name  
Booz Allen Hamilton  
Address: 1234  
City: Springfield  
State: Connecticut  
Country: US and A  
Postal Code: 12345

### Company Point of Contact Information

[Edit](#)

Record #1

Last Name: Coyote  
First Name: Wiley  
Position/Title: Asdf  
Work Telephone: 1112223333  
Email Address: wec@acmerockets.mil  
Time Zone: (GMT+3:30) Tehran

## Incident Information

Edit

### Date Incident Occurred:

Date: 06/02/2024 12:00PM

Time Zone: (GMT-5:00) Eastern Time (US & Canada), Bogota, Lima

### Date Incident Discovered:

Date: 06/05/2024 12:00PM

Time Zone: (GMT-5:00) Eastern Time (US & Canada), Bogota, Lima

### Location(s) of Compromise:

Incident Location CAGE Code(s): 12345

Detection Method: Internally Developed/Proprietary Solutions

Type of Incident: Unknown

Incident Outcome: Unknown

### Incident Mitigation Date:

Date: 06/06/2024 12:00PM

Time Zone: (GMT-5:00) Eastern Time (US & Canada), Bogota, Lima

Incident Narrative (Chronological explanation of incident, threat actor TTPs, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred): asdfasdf

## Supplemental Incident Information

Edit

Was U.S. Government or Military PII compromised or potentially compromised in the cyber incident? Unknown

Known Advanced Persistent Threat (APT) Involved: Unknown

Incident Detected by DC3/DCISE Indicator: No

Any additional information relevant to the incident not included above (Note: This response may contain attributional or sensitive information. It is for DC3/DCISE use only.):

Has this information been shared with any other Federal Government agency? No

Enter any other tracking numbers and the associated point of contact (if applicable):

## Ancillary Information/Questions

Edit

Does this report include known or potentially sensitive Personally Identifiable Information (PII)? No

Do you authorize DC3 to provide this report with attribution to DCSA? Yes

Do you have malicious software related to the cyber incident ready for submission to DC3/DCISE? No

*Malware may be submitted using the Malware portal (link to: <https://ems.dc3on.gov/>)*

**i** I hereby certify that the contents of the report are accurate to the best of my knowledge and verify their authenticity.

Certify Voluntary Cyber Threat Information Sharing/Indicator Only Report \*

Previous

Cancel

Save and Exit

Submit

