



### DIB CS Program Participants Login

#### Report a Cyber Incident

Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#).

Report a Cyber Incident

#### Apply to DIB CS Program

Cleared defense contractors apply to join the DIS CS Program for voluntary cyber threat information sharing. Access requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#).

Apply to Program

#### Login to the DIB CS Information Sharing Portal

Current DIS CS Program participants login to the DIBNet portal. Access requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#).

016 CS Program Participants Log11

- U.S. Department of Defense (DoD)
- DoD Chief Information Officer (CIO)
- DoD Cyber Crime Center (DC3)
- Defense Security Service (DSS)
- Department of Homeland Security (OHS) Enhanced Cybersecurity Services (ECS)
- Defense Security Information Exchange (DSIE)

- [Contact](#)
- [Reporting a Cyber Incident](#)
- [About the 016 CS Program](#)

- [Inspector General](#)
- [Privacy & Security](#)
- [Link Disclaimer](#)
- [Recovery Act](#)
- [FOIA](#)
- [USA.gov](#)
- [No FEAR Act](#)
- [Plain Writing Act of 2010](#)
- [Accessibility/Section 508](#)



Welcome to the DoD & Cyber Threat Info

Home Contact Reso

0704-0489  
XXXXXXXX

Text only version

Apply or Login

Select a certificate

Select a certificate to authenticate yourself to dcise.cert.org:443

Subject	Issuer
OSD.NCR.OOD-QO.MBX.DIB-CS-IA-PRO...	DOD EMAIL CA-28

Certificate information Cancel



### DIB CS Program Participants Login



#### Report a Cyber Incident

Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

Report a Cyber Incident



#### Apply to DIS CS Program

Cleared defense contractors apply to join the DIS CS Program for voluntary cyber threat information sharing. Access requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

Apply to Program



#### Login to the DIS CS Information Sharing Portal

Current DIS CS Program participants login to the DIBNet portal. Access requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

016 CS Program Participants Log11

- U.S. Department of Defense (DoD)
- DoD Chief Information Officer (CIO)
- DoD Cyber Crime Center (DC3)
- Defense Security Service (DSS)
- Department of Homeland Security (OHS) Enhanced Cybersecurity Services (ECS)
- Defense Security Information Exchange (DSIE)

- Contact
- Reporting a Cyber Incident
- About the DIB CS Program

- Inspector General
- Privacy & Security
- Link Disclaimer
- Recovery Act
- FOIA
- USA.gov
- No FEAR Act
- Plain Writing Act of 2010
- Accessibility/Section 508



## 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 **(IE)** 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, **IE** 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. 2224, 44 U.S.C. 3544, HSPD 7, OoO 3020.40, OoO 5505.13E, Door 3020.45, and Door 5205.13.

**Purpose:** Administrative management of the 018 CS/IA Program's information sharing activities. Personal information is covered by OSO SORN OCIO 01, Defense Industrial Base (orB) Cyber Security/Information Assurance Records.

**Routine Use(s):** The OoO Blanket Routine Uses found at <http://dpclo.defense.gov/privacy> apply to this collection. Of those blanket routine uses, we anticipate the following two would most likely be used:

- OoO Blanket Routine Use 01 (Law Enforcement Routine Use). If a system of records maintained by a OoO 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.
- OoO Blanket Routine Use 14 (Counterintelligence Purpose Routine Use). A record from a system of records maintained by a OoO Component may be disclosed as a routine use outside the OoO 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:** Voluntary. However, failure to provide requested information may limit the ability of the OoO to contact the individual or provide other information necessary to facilitate this 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 OoD Directive 5400.07 and OoD 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., 018 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.

Agree  Disagree ]

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.

Unclassified for Official Use Only (When Filled Out)



## Defense Industrial Base (DIB) Cyber Incident Reporting

0704-0489  
XXXXXXXX

### Incident Collection Format

The Incident Collection Format (ICF) is used by OoO contractors to report cyber threat information. Cyber incident reports by OoD contractors are stored in accordance with the *Defense Industrial Base (018) Cybersecurity Activities System of Record Notice*.

#### Routine Uses:

- Voluntary 018 Cybersecurity Activities Use: Share cybersecurity threat information and best practices to enhance and supplement 018 participants' capabilities to safeguard DoO unclassified information that resides on, or transits 018 unclassified information systems.
- Law Enforcement Routine Use: If a system of records maintained by a DoO 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 OoO Component may be disclosed as a routine use outside the OoO 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.

#### User Instructions:

The ICF offers several cyber incident reporting options: Mandatory Cyber Incident reporting (reporting required by contract language including Cloud Service Provider requirements or under the National Industrial Security Program (NISP)); Voluntary Cyber Threat Information sharing; and, Cyber Threat Indicator Only sharing. Upon selection of an incident reporting type, you will be directed to the appropriate collection format.

Following the completion of the ICF, a preview of the incident details will be provided for review and edit. Review the summary page for completeness before confirming reporting submission. *Keep* a record of the reporting submission ID number. Hit "Submit" when you have completed the report format.

The process for submitting a follow-on report is the same as an initial reporting submission. Select the incident report type, select "Yes" to the follow-on reporting question, enter the ICF/reporting submission ID number from the previous submission, and complete all other reporting fields as *needed*. It is important to include the original ICF/reporting submission ID number in order to identify the reporting submission as a follow-on.

Select an option from the reporting types listed below:

- **Mandatory Incident Report**: Select this option if this reporting satisfies a contractual requirement.
- **Cloud Service Provider Incident Report**: Select this option if this reporting satisfies a Cloud Service Provider reporting requirement.
- **Voluntary Cyber Threat Information Sharing/Indicator Only Report** - Select this option for voluntary cyber threat information sharing or indicator only reporting.

Unclassified for Official Use Only (When Filled Out)

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



# Defense Industrial Base (DIB) Cyber Incident Reporting



0704-0489  
XXXXXXXX

## Incident Collection Format

General Information    I. Cyber Incident Report Information    II. Incident Information    Supplemental Incident Information    III. Ancillary Information    Previous

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

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

*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). DCI/DCISC will use the information to prepare analytic products or response actions that do not assign attribution to the originator. e.g., information regarding threats, vulnerabilities, best practices, etc.*

*Non attribution products developed by DCI/DCISC will be disseminated to Federal Government Agencies and participants in the voluntary DoD-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 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., DIS 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.*

Questions marked with \* are required.

### General Information Collection

\* Are you a participant in the 018 CS/1A Program?  
 Yes  No

Is this an Indicator Only submission?  
 Yes  No

\* Is this a follow-on report? (?:  
 Yes  No

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

Enter Other Government Tracking Numbers (if applicable)

Cancel

Next





# Defense Industrial Base (DIB) Cyber Incident Reporting



0704-0489  
XXXXXXXX

## Incident Collection Format

General Information

I. Cyber Incident  
Report Information

II. Incident  
Information

Supplemental  
Incident Information

III. Ancillary  
Information

Preview

### Company Identification Information

\* Company Name

### Company Point of Contact Information *(Page 1)*

\* Last Name  \* First Name

\* Title/Position

\* Address

\* City  \* State  \* Postal Code

\* Telephone  \* Email Address  \* Time Zone

Add Additional Point of Contact

Yes  No



# Defense Industrial Base (DIB) Cyber Incident Reporting



0704-0489  
XXXXXXXX

## Incident Collection Format

- General Information
- I. Cyber Incident Report Information**
- II. Initial Information
- Supplemental Incident Information
- III. Ancillary Information
- Private

### Incident Information

Date Incident Discovered

CS Hour  8 Time Zone

Date incident Occurred

CS Hour  B Time Zone

Location(s) of Incident

\* Incident location CAGE Code (If not applicable, enter N/A)

Incident Outcome

Date incident Resolved

Hour  8 Time Zone

Detection Method

\* Type of incident

\* Incident/Indicator Details/Narrative (including insertion of relevant indicators)  
 For O18 CS/IA Program participants, the information included in this field will be shared in the Participant report. Please do not include attributional or sensitive information, [?]





# Defense Industrial Base (DIB) Cyber Incident Reporting



0704-0489  
XXXXXXXX

## Incident Collection Format

- General Information
- I. Cyber Incident Report Information
- II. Incident Information
- Supplemental Incident Information
- III. Ancillary Information
- Preview

### Supplemental Incident Information

Was PJI compromised or potentially compromised in the occurrence?

- Yes
- No
- Potentially
- Not Determined

Description of technique or method used in incident(s).

[ Choose ]

Known 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.)

Cancel

Previous

Next



# Defense Industrial Base (DIB) Cyber Incident Reporting



0704-0489  
XXXXXXXX

## Incident Collection Format

General Information

I. Cyber Incident Report Information

II. Incident Information

Supplemental Incident Information

III. Ancillary Information

Previous

### Ancillary Information /Questions

- Does this report include known or potential sensitive Personally Identifiable Information (PII)?  
 Yes  No
- Do you authorize DC3 to provide this report with attribution to DSS?  
 Yes  No
- Has Malicious software related to the cyber incident been isolated and ready for submission to DC3/DCISE? *The malware submission form may be accessed through the link provided on the Results page once the /CF has been submitted.*  
 Yes  No

Cancel

Previous

Next





# Defense Industrial Base (DIB) Cyber Incident Reporting



## Incident Collection Format

[General Information](#)
[I. Cyber Incident Report Information](#)
[II. Incident Information](#)
[Supplemental Incident Information](#)
[III. Ancillary Information](#)
[Preview](#)

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

You entered following information:

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

#### General Information Collection

Edit

Are you a participant in the DIB CS/IA Program? **Yes**  
 Is this an Indicator Only submission? **No**  
 Is this a follow-on report? **No**  
 Has this information been shared with any other Federal Government agency? **No**

#### Cyber Incident Report Information

#### Company Identification Information

Edit

Company Name: **dingo inc**  
  
 Company Point of Contact Information  
**Contact #1**  
 Last Name: **non**  
 First Name: **non**  
 Title/Position: **non**  
 Address: **non**  
 city: **no**  
 State: **n**  
 Postal Code: **00000**  
 Telephone: **00000000**  
 Email Address: **asd@ads.com**  
 Time Zone: **EASTERN STANDARD TIME**

#### Incident Information

Incident Location CAGE Code (If not applicable, enter 'N/A'): **00000**  
 Type of incident: **Unauthorized Access**  
 Incident/Indicator Details/Narrative (including insertion of relevant indicators). For DIB CS/IA Program participants, the information included in this field will be shared in the Participant report. Please do not include attributional or sensitive information: **N/A**

Edit

#### Supplemental Incident Information

Known APT Involved: **Unknown**

Edit

#### Ancillary Information/Questions

Does this report include known or potential sensitive Personally Identifiable Information (PII)? **No**  
 Do you authorize DC3 to provide this report with attribution to DSS? **No**  
 Do you require pre-publication review of the Customer Response Form (CRF)? **No**  
 Has malicious software related to the cyber incident been isolated and ready for submission to DC3/DCISE? **No**

Edit

Cancel

Previous

Next