Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) Program

Incident Collection Form

UNCLASSIFIED//FOR OFFICIAL USE ONLY (when filled in)

Welcome to the DIB CS/IA Incident Collection Form

*Authorities:*10 U.S.C. 2224, 44 U.S.C. 3544; HSPD 7; DoDDs 3020.40, 5505.13E, and DoDIs 3020.45 and 5205.13.

Purpose: To enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD unclassified information that resides on, or transits DIB unclassified information systems. DoD Cyber Crime Center (DC3) personnel in the DoD-DIB Collaborative Information Sharing Environment (DCISE) analyze the cyber threat and vulnerability information reported on the Incident Collection Form to develop effective response measures and improved understanding of advanced cyber threat activity. DoD may work with a DIB participant on a more detailed, digital forensics analysis or cyber intrusion damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected information systems, networks, or information. Point of contact information will be stored in the Defense Industrial Base (DIB) Cyber Security/Information Assurance Records system of records.

Routine Uses: DIB participant point of contact information may be provided to other DIB companies to facilitate the sharing of information and expertise related to the DIB CS/IA program, cyber threat information and best practices, and mitigation strategies. The "DoD Blanket Routine Uses" are set forth at http://dpclo.defense.gov/privacy. Of those blanket routine uses, we anticipate the following two would most likely be used:
DoD Blanket Routine Use 01 (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.
DoD Blanket Routine Use 14 (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: 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.

This Incident Collection Form (ICF) is for the submission of network incident information to the DC3/DCISE. To facilitate analysis of intrusion/incident data, please answer questions as completely and accurately as possible. This form is used to submit Initial Incident, Follow-on and Indicator Only reports.

- Please submit an *Initial Incident* report within 72 hours of identification of a cyber incident. Please provide as much information as is available.
- Please submit a *Follow-on* report as additional information on the cyber incident becomes available.
- Please submit an *Indicator Only* report for suspicious cyber activity that is deemed important, but does not meet the level of a cyber incident.

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.

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.). Respondents should identify attribution information in the ICF's fields identified as "For DC3/DCISE Use Only." The U.S. Government may use information that does not assign attribution to the originator (e.g., information regarding threats, vulnerabilities, best practices, etc.) in analytic products or response actions to assist U.S. Government and non-Government partners in protecting their information systems.

Fields are marked either "***For DC3/DCISE-Use Only***", or "***This information will be shared***."

The online ICF is the primary means by which DIB participants submit threat information to the DC3/DCISE. Access to the online ICF is restricted to users with a valid DoD or DoD External Certification Authority (ECA) PKI Identification Certificate. Should a respondent experience difficulty accessing the online Incident Collection Form, please contact the DC3/DCISE hotline at (877) 838-2174 to facilitate exchange of the incident information.

****ICF NOTICE REGARDING PRE-PUBLICATION REVIEW OF CRF****
The originator of an ICF may select whether they want to review a Customer Response Form (CRF) prior to release to the other DIB participants. This option can be found under Section III of the ICF, titled "Incident Information."
If "No" is selected, the originator will NOT be contacted for comments on the CRF prior to release.
If "Yes" is selected, the originator has two (2) federal business days to review the final CRF and respond to DC3/DCISE with instructions on further dissemination of the information before the threat activity and mitigation strategies are released to the other DIB participants and Government stakeholders.
If no response is received by the deadline, DC3/DCISE will distribute the CRF on the third federal business day.

Indicate here whether this is an Initial Incident, Follow-on, or Indicator Only Report help

(This information will be shared.)

• Initial Incident	Select this option for initial incident reporting
• Follow-on Report	Select this option for follow-on reporting
• Indicators Only	In some situations the submitter would like to provide information that may be of interest to DoD and other DIB participants. Select this option for indicator only reporting, and complete only the indicator part of the form.

Does this incident include known or potential **Personally Identifiable Information** (PII)? **help**

(For DC3/DCISE Use Only)

- Yes
- No

Incident Summary Information

In order for us to respond appropriately, please answer the questions as completely and accurately as possible.

II. DIB Participant Points of Contact

Please provide point of contact information to facilitate DC3/DCISE engagement on this incident. The DIB participant point of contact is a cleared individual previously identified and authorized by their DIB company to work directly with DC3/DCISE on cyber threat incident reporting and response.

Incident Report Submitter Contact Information

Last Name help
(For DC3/DCISE Use Only)

First name help
(For DC3/DCISE Use Only)

Email help
(For DC3/DCISE Use Only)

Company Name help
(For DC3/DCISE Use Only)

Location help
(For DC3/DCISE Use Only)

Phone help
(For DC3/DCISE Use Only)

Fax help
(For DC3/DCISE Use Only)

Division / group *help*
(For DC3/DCISE Use Only)

Timezone *help*
(For DC3/DCISE Use Only)

Provide additional POC information as appropriate

At the discretion of the DIB participant, additional POCs that have information on the reported incident may be provided. Please select the appropriate category (i.e., incident response or technical point of contact) and a new window with the same fields as above will appear.

- Incident Response Point of Contact

  The incident response point of contact is the individual who is directly responsible for response and analysis efforts for the incident. If this individual is the same person as the DIB incident report submitter, you do not need to complete this section.

- Technical Point of Contact

  The technical point of contact is the systems administrator who is responsible for the technical management and operation of the affected system(s). If this individual is the same person as the DIB incident report submitter, you do not need to complete this section.

Incident Response Point-of-Contact Information (Optional)

The incident response point of contact is the individual who is directly responsible for the response and analysis efforts for the incident. If this individual is the same person as the DIB incident report submitter, you do not need to complete this section.

Last Name help
(For DC3/DCISE Use Only)

First name help
(For DC3/DCISE Use Only)

Email help
(For DC3/DCISE Use Only)

Company Name help
(For DC3/DCISE Use Only)

Location help
(For DC3/DCISE Use Only)

Phone help
(For DC3/DCISE Use Only)

Fax help
(For DC3/DCISE Use Only)

Division / group *help*
(For DC3/DCISE Use Only)

Timezone *help*
(For DC3/DCISE Use Only)

Technical Point-of-Contact Information (Optional)

The technical point of contact is the system administrator who is responsible for the technical management and operation of the affected system(s). If this individual is the same person as the DIB incident report submitter, you do not need to complete this section.

Last Name help
(For DC3/DCISE Use Only)

First name help
(For DC3/DCISE Use Only)

Email help
(For DC3/DCISE Use Only)

Company Name help
(For DC3/DCISE Use Only)

Location help
(For DC3/DCISE Use Only)

Phone help
(For DC3/DCISE Use Only)

Fax help
(For DC3/DCISE Use Only)

Division / group *help*
(For DC3/DCISE Use Only)

Timezone *help*
(For DC3/DCISE Use Only)

III. Incident Identification

Incident Collection Form (ICF) number (This will be auto-generated if left blank) help
(This information will be shared)

Reporting timestamp (UTC) (This will be auto-generated and read only) help
(This information will be shared)

Partner tracking or incident number help
(For DC3/DCISE Use Only)

Disseminate partner tracking number? Help

- Yes - Tracking number will be shared with partners
- No - Do not share with partners

Other government organization tracking numbers help
(For DC3/DCISE Use Only)

Do you require pre-publication review of the Customer Response Form (CRF)? help
(For DC3/DCISE Use Only)

- Yes
- No

Incident Detail Information

IV. Report Submission Tier and Categorization

Describe the significance of this incident by selecting one of the following options below. help
(This information will be shared)

- **Tier 1a – APT and DoD systems or data involved**
- **Tier 1b – APT and systems or data unknown**
- **Tier 1c – APT and no DoD systems or data involved**
- **Tier 2 – Successful DoD program targeted intrusion, non-APT, encompassing activities that do not fall into Tier 1**
- **Tier 3 – Incidents that do not fall into Tiers 1 or 2 and may be of interest to the cyber community**
- **Not determined at this time.**

Categorize this incident by selecting as many of the following options as apply. help
(This information will be shared)

- **CAT 0 – Situational awareness only**
- **CAT 1 – Root level intrusion**
- **CAT 2 – User-level intrusion**
- **CAT 3 – Unsuccessful activity attempt**
- **CAT 4 – Denial of service**
- **CAT 5 – Non-compliance activity**
- **CAT 6 – Reconnaissance**
- **CAT 7 – Malicious logic**
- **CAT 8 – Investigating**
- **CAT 9 – Explained anomaly**

Provide any additional information to explain how the tier/categories were determined.
help **(This information will be shared)**

Incident impact. help

(This information will be shared)

- **None: no adverse effect**
- **Low: limited adverse effect**
- **Moderate: serious adverse effect**
- **High: severe or catastrophic adverse effect**
- **Unknown**

Does Section IV Report Submission Tier and Categorization contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

V. Incident Description

Please provide a detailed description this incident. This response may contain attribution or sensitive information. help
(For DC3/DCISE Use Only)

Please provide a description of the attack method which may be shared outside of DC3/DCISE. help
(This information will be shared)

Does Section V Incident Description contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

VI. Data Compromise Details

Was data compromised? help
(For DC3/DCISE Use Only)

- Yes
- No
- Unknown

If known, select all compromise types that apply. help
(For DC3/DCISE Use Only)

- **Data confidentiality (e.g., data was viewed or exfiltrated)**
- **Date integrity (e.g., data was altered)**
- **Data availability (e.g., access to data was prevented, DDOS)**
- **Data loss (i.e., data deleted)**

If the data was compromised, is the data associated with a DoD component or program? help
(For DC3/DCISE Use Only)

- Yes
- No
- Not determined

If the answer to previous question is yes, identify the DoD component and/or Program? (e.g., Military Department/Program) help
(For DC3/DCISE Use Only)

Type of information affected (e.g., financial, human resources, etc.) help
(For DC3/DCISE Use Only)

Does Section VI Data Compromise Details contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

VII. Additional Information

Does the attack vector identified appear in Open Source research? help
(This information will be shared)

- Yes
- No
- Unknown

Does this activity represent a shift in TTPs from previously known APT profiles? help
(This information will be shared)

- Yes
- No
- Unknown

Approximate staff time to recover. help
(This information will be shared)

Would you like to provide information regarding observations (e.g., detection, response, indicators, nodes)? help

- Yes
- No

Observation Information (Supplemental)

In order for DC3/DCISE to respond appropriately, please answer the questions as completely and accurately as possible.

I. Incident Observation

Observation Number (Auto-generated)
(This information will be shared)

Reporting timestamp (UTC) (Auto-generated)
(This information will be shared)

Partner observation identification help
(For DC3/DCISE Use Only)

Please provide a detailed description of this observation. This response may contain attribution or sensitive information. help
(For DC3/DCISE Use Only)

Please provide a detailed description of this observation which may be shared outside the DC3/DCISE. help
(This information will be shared)

Does Section I Incident Observation contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

II. Incident Information – Detection and Response

Detection Method (Select all that apply)
(This information will be shared)

- Email Gateway Monitoring
- Honeypot / Decoy Device
- Anti-virus / Anti-Malware
- Log Review
- Proactive Detection / Audit
- Host-based IDS
- Network-based IDS
- Internet Proxy Monitoring
- Security Event and Information Manager
- Network-based IPS
- User Interface / Browser
- Host-based IPS
- ISP Operated Sensor
- Human
- Other

Outcome (Please select one)

(This information will be shared)

- **Successful Compromise**
- **Failed Attempt**
- **Unknown**

Response Actions (Select all that apply)

(This information will be shared)

- **No action taken**
- **Contacted target site**
- **Investigating**
- **Blocked source network**
- **Rate limit from source host**
- **Rate limit network protocol port**
- **Triaging reports**
- **Contacted attach source site**
- **Contacted originator**
- **Blocked host**
- **Blocked network protocol port**
- **Rate limit traffic from source network**
- **Receiving additional information**
- **Other**

Incident start date and time
(This information will be shared)

Incident start timezone
(This information will be shared)

Incident observation date and time
(This information will be shared)

Incident observation timezone
(This information will be shared)

Incident resolution date and time
(This information will be shared)

Incident resolution timezone
(This information will be shared)

Do you have media or malware that you will be submitting for DC3/DCISE analysis?

help

(For DC3/DCISE Use Only)

- Yes
- No

Were specific systems targeted or malicious/attacking systems identified? help

(For DC3/DCISE Use Only)

- Yes
- No

Was this activity detected by a DC3/DCISE-provided indicator?

(This information will be shared)

- Yes
- No

Host Information (Supplemental)

This section is used to provide individual host information. Answer **Yes** to the last question in this section to continue entering host information. Answer **No** to the last question when you have completed entering host information.

Host Information – Supplemental

Host Tracking Number (Auto-generated)
(For DC3/DCISE Use Only)

Reporting timestamp (UTC) (Auto-generated)
(For DC3/DCISE Use Only)

Partner host identification help
(For DC3/DCISE Use Only)

Was this a targeted host or malicious/attacking host? help
(For DC3/DCISE Use Only)

IP address or IP address range (e.g., xxx,xxx,xxx,xxx (IP address) or xxx.xxx.xxx.xxx-zzz.zzz.zzz.zzz (IP address range) help
(For DC3/DCISE Use Only)

System name or system names help
(For DC3/DCISE Use Only)

DNS name or DNS names (e.g., SystemName.DomainName.com) help
(For DC3/DCISE Use Only)

If you know what time you resolved the target system, please provide that information. help
(For DC3/DCISE Use Only)

(For DC3/DCISE Use Only) *Please select a time zone.*

Is the affected system/node (or service) significant to the operation of the organization or infrastructure? help
(For DC3/DCISE Use Only)

- Yes
- No
- Unknown

Host Functions (Please select all that apply) help

- End user system
- Peer-to-peer node
- Corporate application server
- Web content server
- Authentication server (e.g., Kerberos, Active Directory)
- Engineering/ development
- Publicly accessible server
- Directory server (e.g., LDAP, whois)
- Hardware/ software release or repository
- Instant messaging server
- Application server
- Business development or sale system
- Email server
- Print server
- Manufacturing controller
- Voice (e.g., SIP, H.323)
- Infrastructure (e.g., router, firewall)
- Marking system
- Streaming-media server
- Database server
- License server
- File Transfer Protocol (FTP) server
- Unknown
- Sensor
- File server (e.g., SMB, AFS, SVN)
- Log server
- Internal-use-only server
- Name server (e.g., DNS, WINS)
- Lab or development system
- Other

Host Operating System (major) help

(For DC3/DCISE Use Only)

- Microsoft Windows
- UNIX/Linux
- Apple Mac OS
- Unknown
- Other

Host Operating System version. help

(For DC3/DCISE Use Only)

Is this a virtual machine? help

(For DC3/DCISE Use Only)

- Yes
- No
- Unknown

If yes to question above, were virtual machines affected by this event? help

(For DC3/DCISE Use Only)

- Yes
- No
- Unknown

Host State (select all that apply). help

- **Spoofed**
- **Innocent, Compromised**
- **Fraudulent**
- **Innocent, Hijacked**
- **Unknown**
- **Other**

Physical location of the node. help

(For DC3/DCISE Use Only)

CAGE code. help
(For DC3/DCISE Use Only)

If there is additional information about this node that is relevant to this incident, please provide. help
(For DC3/DCISE Use Only)

Are there additional targeted or attacker systems? help

- Yes
- No

Does Section Host Information - Supplemental contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

Indicator Information (Supplemental)

This section is used to provide indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

Indicator Type Information – Supplemental

What type of indicators would you like to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- I can provide a block of indicators in approved CSV format
- None

Network Indicator Information (Supplemental)

This section is used to provide Network Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

Network Indicators – Supplemental

help

Indicator Type
(This information will be shared)

- Network Indicators

Indicator Sub-Type
(This information will be shared)

- IPv4Address
- IPv4RangeStart
- IPv4RangeEnd
- IPv6Address
- IPv6RangeStart
- IPv6RangeEnd
- Application protocol
- Port
- Protocol
- Encryption Type
- Whois
- FQDN

Value
(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)
(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)
(This information will be shared)

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section Network Indicators - Supplemental contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

Signature Indicator Information (Supplemental)

This section is used to provide Signature Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

Signature Indicators – Supplemental

help

Indicator Type

(This information will be shared)

- Signature Indicators

Indicator Sub-Type

(This information will be shared)

- SignatureType
- SignatureString

Value

(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)

(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)

(This information will be shared)

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section Signature Indicators - Supplemental contain known or potential PII?

(For DC3/DCISE Use Only)

- Yes
- No

Registry Indicator Information (Supplemental)

This section is used to provide Registry Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

Registry Indicators – Supplemental

help

Indicator Type
(This information will be shared)

- Registry Indicators

Indicator Sub-Type
(This information will be shared)

- RegistryHive
- RegistryKeyValue
- RegistryKeyPath

Value
(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)
(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)
(This information will be shared)

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section Registry Indicators - Supplemental contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

Email Indicator Information (Supplemental)

This section is used to provide Email Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

Email Indicators – Supplemental

help

Indicator Type
(This information will be shared)

- Email Indicators

Indicator Sub-Type
(This information will be shared)

- Subject
- SenderDisplayName
- Sender
- DownstreamIPAddress
- SenderIP
- Message-ID
- Header
- EmailStringGeneral

Value
(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)
(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)
(This information will be shared)

Are there additional indicators to report? help

- Network
- String
- Signature
- None
- Registry
- Email
- File

Does Section Email Indicators - Supplemental contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No

File Indicator Information (Supplemental)

This section is used to provide File Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

File Indicators – Supplemental

help

Indicator Type

(This information will be shared)

- File Indicators

Indicator Sub-Type

(This information will be shared)

- FileAccessedTime
- FileChangedTime
- FileCompileTime
- FileCreatedTime
- FileExtension
- FileFullPath
- FileMD5
- FileModifiedTime
- Filename
- FileOwner
- FileSize
- FileStrings
- FileSHA1
- FileSSDeep
- CompressionType
- Malicious (Y/N)
- MalwareType
- MalwareFamily

Value

(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)

(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)

(This information will be shared)

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section File Indicators - Supplemental contain known or potential PII?

(For DC3/DCISE Use Only)

- Yes
- No

String Indicator Information (Supplemental)

This section is used to provide String Indicator information. Please provide as much information as possible. Continue to select indicator types until complete, then select "None."

String Indicators – Supplemental

help

Indicator Type

(This information will be shared)

- String Indicators

Indicator Sub-Type

(This information will be shared)

- AutonomousSystemNumber
- ATMAddress
- MACAddress
- UniformResourceLocator (URL)
- ServiceName
- Other

Value

(This information will be shared)

Description (This response may contain attribution or sensitive information. It is internal, for DC3/DCISE use only.)

(For DC3/DCISE Use Only)

Description (This response may include information which may be shared outside the DC3/DCISE.)

(This information will be shared)

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section String Indicators - Supplemental contain known or potential PII?

(For DC3/DCISE Use Only)

- Yes
- No

Bulk Indicator Information (Supplemental)

This section is used to provide Indicator information in bulk CSV format. Please ensure the data is in the approved CSV format; there is a limit of 16,000 characters. Continue to select indicator types until complete, then select "None."

Indicator Bulk Data – Supplemental

help

Indicator Type

(This information will be shared)

- Indicator Bulk Data

Indicator Data (CSV) help

(This information will be shared)

Indicator Type, Indicator Sub-Type, Indicator Value, *Description – Private*, Description - Shared

Are there additional indicators to report? help

- Network
- Signature
- Registry
- Email
- File
- String
- None

Does Section Bulk Indicators - Supplemental contain known or potential PII?

(For DC3/DCISE Use Only)

- Yes
- No

Indicators Only Summary Information

In order for DC3/DCISE to respond appropriately, please answer the questions as completely and accurately as possible.

I. DIB Participant Point of Contact

Please provide point of contact information to facilitate DC3/DCISE engagement on this incident. The DIB participant point of contact is a cleared individual previously identified and authorized by their DIB company to work directly with DC3/DCISE on cyber threat incident reporting and response.

Incident Report Submitter Contact Information

Last Name help
(For DC3/DCISE Use Only)

First name help
(For DC3/DCISE Use Only)

Email help
(For DC3/DCISE Use Only)

Company Name help
(For DC3/DCISE Use Only)

Location help
(For DC3/DCISE Use Only)

Phone help
(For DC3/DCISE Use Only)

Fax help
(For DC3/DCISE Use Only)

Division / group *help*
(For DC3/DCISE Use Only)

Timezone *help*
(For DC3/DCISE Use Only)

Provide additional POC information as appropriate

At the discretion of the DIB participant, additional POCs that have information on the reported incident may be provided. Please select the appropriate category (i.e., incident response or technical points of contact) and a new window with the same fields as above will appear. .

- Incident Response Point of Contact — The incident response point of contact is the individual who is directly responsible for response and analysis efforts for the incident. If this individual is the same person as the DIB incident report submitter, you do not need to complete this section. If the incident response point of contact is a different person, complete the following fields.
- Technical Point of Contact — The technical point of contact is the systems administrator who is responsible for the technical management and operation of the affected system(s). If this individual is the same person as the DIB incident report submitter, you do not need to complete this section. If the technical point of contact is a different person, complete the following fields.

II. Indicator Description

Incident Collection Form (ICF) number (This will be auto-generated if left blank) help
(This information will be shared)

Do you require pre-publication review of the Customer Response Form (CRF)? help
(For DC3/DCISE Use Only)

- Yes
- No

Does this incident involve known or potential Personally Identifiable Information (PII)? help
(For DC3/DCISE Use Only)

- Yes
- No

Please provide a detailed description this incident. This response may contain attribution or sensitive information. help
(For DC3/DCISE Use Only)

Please provide a description of the attack method which may be shared outside of DC3/DCISE.
help (This information will be shared)

Does this Indicator Only Summary contain known or potential PII?
(For DC3/DCISE Use Only)

- Yes
- No