Defense Industrial Base (DIB) Cyber Incident Reporting

The DIB Cyber Incident Collection Format (ICF) is the primary means by which DoD contractors report cyber incident information to DoD. Access to the online ICF is restricted to users with a DoD-approved Public Key Infrastructure (PKI) certificate. Should a respondent experience difficulty accessing the online ICF, please contact the DC3/DCISE hotline at (877) 838-2174 to facilitate exchange of the incident information.

General Information Collection

- Does this report include known or potential sensitive Personally Identifiable Information (PII)?
- Is this a follow-on report? (check appropriate box)
  - € Yes
  - € No
- Enter ICF Number of Initial Report (if applicable)
- Has this information been shared with any other Federal Government agency?
  - € Yes, please specify:_____
  - € No
- Enter Other Tracking Numbers (if applicable)

Section I: Company Identification Information

- Company Name:
- Data Universal Numbering System (DUNS):
- Facility Commercial And Government Entity (CAGE) code:
- Facility clearance level (if applicable):
  - € Unclassified
  - € Confidential
  - € Secret
  - € Top Secret
  - € Not Applicable
- Are you a cleared defense contractor?
  - € Yes
  - € No
- Is this a National Industrial Security Program required report (see NISPOM Chapter 3, Sections 1-301, 1-302(b))?
  - € Yes
  - € No
  - € Not Applicable

- Does this incident impact covered defense information?
  - € Yes
  - € No
  - € Unknown
- If yes, identify the type of covered defense information impacted.
  - € Unclassified CTI
  - € Export Controlled information
  - € Critical Information (Operations Security)
  - € Any other information
- Does this incident/compromise impact your company's ability to provide operationally critical support? If yes, please explain.
- Company Point of Contact Information (complete each field)
  - € Name:
  - € Position:
  - € Address:
  - € Telephone:
  - € Email:
  - € Time zone:

Section III. Contract Information or Other Agreement (complete each field, if applicable)

- Contract numbers or other Agreement affected or potentially affected (If a NISP report, enter NISP):
- Contract or other Agreement clearance level
  - € Unclassified
  - € Confidential
  - € Secret
  - € Top Secret
- USG Contracting Officer(s):
  - € Name:
  - € Address:
  - € Position:
  - € Telephone:
  - € Email:
- USG Program Manager point(s) of contact:
  - € Name:
  - € Address:
  - € Position:
  - € Telephone:
  - € Email:

Section IV. Incident Information (complete each field, if applicable)

- Date the incident was discovered:

- Date and time the incident occurred (if known):
- Location(s) of compromise:
- Incident location CAGE Code:
- DoD Programs, Platforms or Systems Involved
- Detection Method
- Type of compromise (select all that apply):
    - € Unauthorized Access
    - € Unauthorized Release (includes inadvertent release)
    - € Other_____
    - € Unknown at this time
    - € Not Applicable

- Description of the technique or method used in cyber incident(s):
    - € Threat vectors (see US-CERT Federal Incident Notification Guidelines) if know, (select all that apply)
        - Unknown
        - Attrition
        - Web
        - Email
        - External/removable media
        - Impersonation/spoofing
        - Improper usage
        - Loss of theft of equipment
        - Other
- Incident outcome
    - € Successful Compromise
    - € Failed attempt
    - € Unknown
- Incident Resolution Date/Time (if applicable)
- Incident/Compromise Narrative (include relevant indicators) - Note: Within the narrative description include relevant information such as adversary IP addresses and domains; targeted IP addresses and domains; web URLs; email headers; email subject; email sender name; email sender address; email originating IP address; email recipient(s); email body; hyperlinks; attached files; other related file names [including both malicious and benign]; related file directory locations; file hashes; Windows registry modifications; malicious code analysis results; and, related network activity.

  Insert indicators here.

- Supplemental Incident Information

- € Known Advanced Persistent Threat (APT) involved
  - Yes
  - No
- € Incident detected by DC3/DCISE indicator?
  - Yes
  - No
- € Any additional information relevant to the incident not included above

Insert information here.

Section IV. Ancillary Information Questions

- Was Personally Identifiable Information compromised in the cyber incident?
- Do you want to submit Media/Malicious Software related to the cyber incident to DC3/DCISE?
- Do you want to make a voluntary Cyber Threat Information Sharing or Indicator Only Report?