Defense Industrial Base (DIB) Cybersecurity (CS) Activities
Incident Collection Form (ICF)
Overview for Office of Management and Budget

Purpose

The purpose of this document is to provide an overview of the Incident Collection Form (ICF) for the Office of Management and Budget. The DIB cyber Incident Collection Form (ICF) is the primary means by which DoD contractors report cyber incidents 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.

Section I. Cyber Incident Report Information

The user chooses the type of submission. This form is used by all DoD contractors to report cyber incidents on unclassified DoD contractor networks.

- Initial Cyber Incident Report Required by DoD Contract or Other Agreement - An initial incident report should be submitted within 72 hours of identification of a cyber incident and provide information in as many fields as available.

- Follow-on Reports - Follow-on reports should be submitted as additional information related to the cyber incident becomes available. The submitter is asked to provide the ICF number of the initial cyber incident report.

- A Voluntary Cyber Incident Report Not Required by Contract or Other Agreement – This report is submitted voluntarily by participants in the DIB CS cyber threat sharing program and includes an “indicator only report” submitted for situational awareness and sharing with other DIB participants.

Section II. Company Identification Information

This section provides information about the company submitting the ICF.

Section III. Company Point of Contact Information

This section identifies Points of Contact (POC) information for the ICF.

Section IV. Contract Information

This section identifies contract(s) that have been affected under the ICF, and the associated USG Contracting Officer and Program Manager POCs. If the submitter is a DoD Cloud Service Provider, they are required to identify the Mission Computer Network Defense (MCND) Service Provider.

Section V. Incident Details

The section allows the submitter to provide details about the incident including date, time and location of the compromise; the Operating System of the affected system; a description of the technique or method used; relevant indicators; mitigating factors and actions relevant to the incident; and prioritization factors for Cloud Services Providers.

Section VI. DoD Programs, Information or Mission Support Affected

This section address the type of covered defense information that was or may have been compromised, or if the cyber incident has impacted the contractor's ability to provide operationally critical support.

Section VII. Supplemental Information

This optional section of the ICF requests the submitter provide additional information relevant to the cyber incident report.

Section VIII. Information Dissemination

This section determines if the information provided has been or may be shared with other USG agencies or participants in the DIB CS/IA voluntary threat information sharing program.

Section IX. Malicious Software

This section allows the submitter to indicate if they have discovered and isolated malicious software for further digital forensic analysis. If the submitter indicates "yes." procedures are provided for submitting a sample of the malicious software to DoD for analysis.