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

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.

Part I. Type of Report Submission

The user chooses the type of submission:

Initial Incident Report - An Initial Incident report should be submitted within 72 hours of identification of a cyber incident, providing information in as many fields where information is available.

Follow-on Reports - Follow-on Reports should be submitted as additional information related to the cyber incident becomes available. The Adobe Acrobat and the web version allow the submitter to identify which ICF is being updated by providing the ICF number (Section III) of the original ICF.

Indicators Only - The option is used to report suspicious cyber activities which the submitter believes are important, but do not meet the level of a cyber incident.

Part II. DIB Point of Contact

The purpose of this section is to identify the person submitting the ICF and contact information. This section also allows the submitter to provide additional Points of Contact (POCs) as needed.

Part III. Incident Identification

The purpose of this section is to assign a unique identifier to the ICF submission for administrative purposes. If the incident has been reported to other Government agencies, this section allows the submitter to provide information on what agency this event was reported to and the associated tracking number. Additionally, the submitter may enter the company internal tracking number, if applicable, which allows for quick cross reference.

Part IV. Report Submission Tier and Categorization

The purpose of this section is for analysis of the submitted ICF. The submitter is asked to indicate if the incident was related to known threats and if DoD information was involved. Submitter is also asked to categorize the type of event and to input text to further describe the incident. The submitter should estimate the impact of the incident, if known.

Part V. Incident Description

The purpose of this section is to allow the submitter to provide details about the incident. This section has two parts. The first section allows the submitter to provide detailed information about the incident, including attribution information that reveals the source of the data (i.e., the submitting company). This section will be used only by DC3/DCISE.

The second section allows the submitter to provide detailed information about the incident without attribution information. This section may be shared with government and DIB stakeholders outside of DC3/DCISE.

Part VI. Data Compromise Details

The purpose of this section is to assess the data compromise type (confidentiality, integrity, etc,), and if known, to identify what DoD program information was affected.

Part VII. Additional Information

The purpose of this section is to gather information not addressed in the other sections. A "yes" answer to the question, "Would you like to provide information regarding observations (e.g., detection, response, indicators, note)?" opens the "Observation" page where the user can submit very detailed information about the observed incident.

Supplemental Information

The submitter may provide supplemental information in the following areas: **Observations**, **Hosts**, **Indicators** by type (Network, Signature, Registry, Email, File, String, Bulk).

Supplemental Information – Observations

An observation is an individual instance of activity that either solely, or in combination with other observations, comprises the entire incident being reported. Observations provide the information necessary to characterize, identify, and contain the activity. Because an incident could have many observations, this supplemental section is designed so that user can provide many observations for each incident.

Part I. Incident Observation

This section is used to describe information about the incident that led to identification and reporting of the incident. It includes how the activity was detected, what actions were taken, when it was observed, etc. This information is more detailed and is useful for forensic analysis. The observation description information has two sections: one section will be used only by the DC3/DCISE and may contain attribution information; the other section is for information that can be shared with others.

Part II: Incident Information – Detection and Response

This section contains a number of options for the submitter to "check all that apply". Because of the rapidly evolving nature of technology, request that DoD be allowed to update the items in the sections Detection Method and Response Actions, as needed, in order to gather the most technically relevant, and up-to-date information.

If specific systems were targeted or malicious/attacking systems identified, then a supplemental information page of the form is presented to the submitter.

Supplemental Information - Hosts
The section is used to gather information about the system(s) involved in the incident. The submitter has the option to provide system specific information such as system name, Internet protocol address, and the system functions (i.e., email server, end user system). Because many hosts may be involved in the incident, the form allows for multiple host submissions.

DoD must be allowed to update the items in section on Host Functions, as needed, in order to gather to most technically relevant, up-to-date information, including changes reflecting rapidly evolving nature of technology.

Supplemental Information - Indicators
The indicator supplemental information is organized by types of indicator: network indicator; signature indicator; registry indicator; email indicator, file indicator, string indicator, and bulk indicator.

Each indicator page follows a standard format to collect information about the indicator type, the associated value, and description in two parts: the first allows the submitter to include attribution/company specific information that is for DC3/DCISE use only; the second section is for detailed information about the indicator without attribution information that may be shared with organizations outside of the DC3/DCISE.

Indicator Only Submission
The **Indicator Only** submission allows the submitter to provide information about suspicious cyber activities that may be important, but do not meet the level of a cyber incident.

Part I. DIB Point of Contact
The Point of Contact information is needed if the submitter elects the indicator only submission. The submitter will have the option of selecting providing additional POC information as needed.

Part II. Indicator Description
The submitter may use Indicator Description to provide more detailed information on this indicator or set of indicators. This description section has two parts: the first allows the submitter to include attribution/company specific information that is for DC3/DCISE use only; the second section is for detailed information about the indicator without attribution information that may be shared with organizations outside of the DC3/DCISE.

If the submitter selects the type of indicator to report (e.g., Network, Email, File), the appropriate supplemental page will open (see descriptions above) allowing the

submitter to provide the type, value, and a description of the indicator. Again, the description is divided into an attribution and non-attribution section.

Additionally, in order to gather the most technically relevant information possible, request DoD be permitted to update, as needed, the “Supplement Information – Indicators” section.

Summary

This form includes fields relevant to today’s technology and cyber forensic techniques. However, due to the rapid changes in information technology and attack vectors, DoD requests OMB permission to update the following sections as needed without issuing a new form. These are:

1) Supplemental Information – Observations: Section II Detection method and response actions
2) Supplemental Information – Host functions
3) Supplemental Information – Indicators: Indicator sub-types