

Request for Records Disposition Authority

Records Schedule Number DAA-0330-2015-0005
Schedule Status Approved

Agency or Establishment Office of the Secretary of Defense
Record Group / Scheduling Group Records of the Office of the Secretary of Defense
Records Schedule applies to Major Subdivision
Major Subdivision CHIEF INFORMATION OFFICER, for the DEPARTMENT OF
DEFENSE (DoD CIO)
Minor Subdivision DOD CYBER CRIME CENTER (DC3)
Schedule Subject DEFENSE INDUSTRIAL BASE (DIB) CYBER SECURITY/
INFORMATION ASSURANCE RECORDS (DIB CS/IA)

Internal agency concurrences will be provided No

Background Information DIB CS/IA is a DoD program designed to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified networks and information systems by sharing cyber threat information and collaboration between DoD and industry.

Item Count

| Number of Total Disposition Items | Number of Permanent Disposition Items | Number of Temporary Disposition Items | Number of Withdrawn Disposition Items |
|-----------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| 3 | 0 | 3 | 0 |

GAO Approval

Outline of Records Schedule Items for DAA-0330-2015-0005

| Sequence Number | |
|-----------------|--|
| 1 | Defense Industrial Base (DIB) Cyber Security/Information Assurance System Data base |
| 1.1 | Defense Industrial Base (DIB) Cyber Security/Information Assurance System Database Master Files Disposition Authority Number: DAA-0330-2015-0005-0001 |
| 2 | Cybersecurity Assessments Disposition Authority Number: DAA-0330-2015-0005-0002 |
| 3 | Cyber Incident Response and Analysis Disposition Authority Number: DAA-0330-2015-0005-0003 |

Records Schedule Items

| Sequence Number | | | | | | | | | |
|---|---|-------------------|-----------|-------------|--------|-----------------------------|-----|---|-----|
| 1 | <p>Defense Industrial Base (DIB) Cyber Security/Information Assurance System Database</p> <p>When cyber incident reports are received, DoD Cyber Crime Center (DC3) personnel analyze the information for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government and DIB understanding of advanced cyber threat activity. DoD may work with a DIB company on a more detailed, digital forensics analysis or damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information. INPUTS: Include but are not limited to Defense Industrial Base (DIB) company point of contact information includes name, company name and mailing address, work division/group, work email, and work telephone number, incident reports received from DIB participants. OUTPUTS: Ad-hoc reports and metrics records created on an ad hoc basis for reference purposes or to meet day-to-day business needs. (GRS 20 Item16) Cyber Incident Response and Analysis, reports consisting of assessments, analysis of cyber incident report data information relevant to the potential or known compromise of DIB partner information systems including trend analysis and extrapolation. (GRS 20, Item 5) SYSTEM INTERFACES: N/A System documentation will be kept in accordance with (GRS 11a(1))</p> | | | | | | | | |
| 1.1 | <p>Defense Industrial Base (DIB) Cyber Security/Information Assurance System Database Master Files</p> <p>Disposition Authority Number DAA-0330-2015-0005-0001</p> <p>The Defense Industrial Base (DIB) Cyber Security/Information Assurance records (DIB CS/IA) are used to assess vulnerabilities and threat to the elements of the defense and supporting non-defense information infrastructures that are essential to the operations of the Department. The master file include but are not limited company point of contact information includes name, company name and mailing address, work division/group, work email, and work telephone number (known as DIB Participant Information), Cyber Intrusion Damage Assessments, including Initial and Follow-up incident reports.</p> <table data-bbox="375 1591 933 1876"><tr><td>Final Disposition</td><td>Temporary</td></tr><tr><td>Item Status</td><td>Active</td></tr><tr><td>Is this item media neutral?</td><td>Yes</td></tr><tr><td>Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?</td><td>Yes</td></tr></table> | Final Disposition | Temporary | Item Status | Active | Is this item media neutral? | Yes | Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing? | Yes |
| Final Disposition | Temporary | | | | | | | | |
| Item Status | Active | | | | | | | | |
| Is this item media neutral? | Yes | | | | | | | | |
| Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing? | Yes | | | | | | | | |

2

Do any of the records covered by this item exist as structured electronic data? **Yes**

Disposition Instruction

Retention Period **Master file consisting of DIB Participant Information: Temporary; Destroy 3 years after the participating company withdraws from the program, closes or goes out of business.**

Additional Information

GAO Approval **Not Required**

Cybersecurity Assessments

Disposition Authority Number **DAA-0330-2015-0005-0002**

Initial, Follow-up incident reports and Cyber Intrusion Damage Assessments

Final Disposition **Temporary**

Item Status **Active**

Is this item media neutral? **Yes**

Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing? **Yes**

Do any of the records covered by this item exist as structured electronic data? **Yes**

Disposition Instruction

Cutoff Instruction **Close files annually**

Retention Period **Destroy 10 year(s) after cut off**

Additional Information

GAO Approval **Not Required**

3

Cyber Incident Response and Analysis

Disposition Authority Number **DAA-0330-2015-0005-0003**

Reports consisting of assessments, analysis of incident report data information relevant to the potential or known compromise of DIB partner information systems including trend analysis and extrapolation.

Final Disposition **Temporary**

Item Status **Active**

| | |
|---|----------------------------------|
| Is this item media neutral? | Yes |
| Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing? | Yes |
| Do any of the records covered by this item exist as structured electronic data? | Yes |
| Disposition Instruction | |
| Cutoff Instruction | Close files annually |
| Retention Period | Destroy 10 year(s) after cut off |
| Additional Information | |
| GAO Approval | Not Required |

Agency Certification

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal in this schedule are not now needed for the business of the agency or will not be needed after the retention periods specified.

Signatory Information

| Date | Action | By | Title | Organization |
|------------|------------------------|------------------|---|---|
| 02/23/2015 | Certify | Luz Ortiz | OSD Records Manager | Department of Defense - Office of the Secretary of Defense |
| 08/10/2015 | Submit for Concurrence | Sebastian Welch | Appraiser | National Archives and Records Administration - Records Management Services |
| 08/10/2015 | Concur | Margaret Hawkins | Director of Records Management Services | National Records Management Program - ACNR Records Management Services |
| 08/11/2015 | Concur | Laurence Brewer | Director, National Records Management Program | National Archives and Records Administration - National Records Management Program |
| 08/12/2015 | Approve | David Ferriero | Archivist of the United States | Office of the Archivist - Office of the Archivist |