Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

## General Information

| | |
|---|---|
| Agency or Establishment | United States Coast Guard |
| Record/Scheduling Group | 0026 - Records of the U.S. Coast Guard |
| Records Schedule Applies To | Agency Subdivision |
| Major Subdivision | Coast Guard Cyber Command |
| Minor Subdivision | CGCC-37 Cyber Protection Team(s) |
| Schedule Subject | Cyber Protection Team (CPT) Analysis Data |
| Additional Schedule Information | The Coast Guard (CG) has authority to prevent, detect, and respond to threats endangering Maritime Critical Infrastructure and Key Resources (CI/KR) entities. The Coast Guard is Co-Sector Risk Management Agency (SRMA) for the Transportation Sector and has responsibility for protecting maritime CI/KR. Coast Guard Cyber Command (CGCYBER), in support of CG Sector Commanders, provides technical assistance to State, Local, Territorial, and Tribal (SLTT) entities by enhancing Maritime Critical Infrastructure cyber resilience (through CPT missions) within their Areas of Responsibility. The typical mission partner is part of the Marine Transportation System (MTS), although not all are. There may be overlap with other US industry sectors, but CPT mission partners have a maritime nexus (they are located within or adjacent to the marine environment). |

| | |
|---|---|
| | Mission-related data resides within the Cyber Protection Team (CPT) Out-of-Band CPT Mission & Analysis Network (OCEAN). Coast Guard Cyber Command (CGCYBER) Cyber Protection Teams (CPTs) were established to offer cybersecurity capabilities to partners in the marine transportation system (MTS). CPT missions generate documents (e.g., out-briefs, technical reports, and field intelligence reports) and raw data that is stored in supporting infrastructure. CPT supports mission partners with hunt or incident response to include Vulnerability Assessments, Threat Hunting, or Cyber Incident Response . Missions vary in duration and may be conducted via a variety of means and do not necessarily entail the deployment of onsite assets. When executing a mission the CPT partners with the local Captain of the Port and operates under their authorities. Through partnership with the Captain of Port, CPT provides technical assistance to an entity with a maritime critical infrastructure nexus. Generally the CPT mission partners are external to both the CG and Federal Government, belonging to private industry in the U.S. A mission concludes when a final report or document has been provided to the mission partner who requested support.<br><br>Records are raw or unprocessed data and duplicate drive images provided to or collected by CPT during team missions that require further analysis to provide finalized products such as Indicators of Compromise (IOCs), Field Intelligence Reports (FIR), and other analytical information such as vulnerability type by geographic location and industry. Raw data includes analytically relevant and non-analytically relevant data. Examples of raw data include unconstructed or raw packet capture (PCAP), IP addresses, file data, domain names, file locations, system logs, network logs or other information deemed relevant to the mission. Reports produced by the mission team as final output including findings and recommendations are provided to the mission partner. Out-of-Band CPT Mission & Analysis Network (OCEAN) is the lab environment in which CPT analysts perform data analysis and correlation against data collected during a mission. On mission, the CPTs obtain metadata from the customer's network with the customer's consent. Coast Guard CPTs conduct a variety of cyber missions to defend the MTS. |
| Is There a Classified Version of This Schedule? | No |

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

| | |
|---|---|
| Is consultation and coordination with Tribal Governments required? | No - the records covered by this schedule do not implicate Tribal interests |

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

## Item Count

Total number of disposition items: 9
Number of Temporary disposition items: 5
Number of Permanent disposition items: 4
Number of Items with Disposition Not Approved: 0
Number of Inactive disposition items: 0

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

## Outline of Records Schedule Items for DAA-0026-2022-0001

| Item # | Title | Disposition |
|---|---|---|
| 0001 | Cyber Protection Team Analysis Data - Non-analytically Relevant Raw Data | Temporary |
| 0002 | Cyber Protection Team Analysis Data - Raw Data of Analytic Value | Temporary |
| 0003 | Story Boards | Temporary |
| 0004 | Indicators of Compromise | Temporary |
| 0005 | Final Technical Reports | Permanent |
| 0006 | Out Briefs | Temporary |
| 0007 | Cyber Trends and Insights in the Marine Environment (CTIME) Reports | Permanent |
| 0008 | Maritime Cyber Communications : Maritime Cyber Alerts (MCA) | Permanent |
| 0009 | Maritime Cyber Communications : Maritime Cyber Bulletins (MCB) | Permanent |

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

## Records Schedule Items

| DAA-0026-2022-0001-0001 | STATUS: Active |
|---|---|
| **ITEM GENERAL INFORMATION** | |
| Item Title | Cyber Protection Team Analysis Data - Non-analytically Relevant Raw Data |
| Item Description | Raw mission-related data that resides within the Cyber Protection Team (CPT) Out-of-Band CPT Mission & Analysis Network (OCEAN) provided to or collected by CPT during team missions that require further analysis to provide finalized products such as Indicators of Compromise (IOCs), Field Intelligence Reports (FIR), and other analytical information such as vulnerability type by geographic location and industry. The raw data is collected by the deployable mission support suite for analysis to determine impacts, such as potential vulnerabilities or malicious cyber activity. Non-analytically relevant data is the portion of data collected that does not contribute to analysis. To collect data CPT analysts place sensors on the mission partners network, with the mission partner's consent. The sensors collect a mirror copy of the data transmitting through the network or through an end point agent that collects a copy of the host machine data. Once the data is collected it is analyzed by CPT analysts and determined to be analytically relevant or not. Non-analytically relevant data is maintained as part of the mission but not shared. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| **MANUAL CITATION** | |
| Agency Code | 047-01-007, Revision # 03 |
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017 |
| **SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS** | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| **DISPOSITION INSTRUCTION** | |
| Final Disposition | Temporary |

| | |
|---|---|
| Cutoff Instructions | Cut off at end of Calendar year. |
| Retention Period | Other: Destroy upon termination or fulfillment of contractual obligations with mission partners, but no later than 1 year after cutoff. |
| ADDITIONAL INFORMATION | |
| Legal citation related to record retention (if applicable) | N/A - USCG Legal Counsel has reviewed the schedule. |
| Are any of the records covered by this item national security classified? | No |
| GAO Approval Required | Requested and Received |

| DAA-0026-2022-0001-0002 | STATUS: Active |
|---|---|
| ITEM GENERAL INFORMATION | |
| Item Title | Cyber Protection Team Analysis Data - Raw Data of Analytic Value |
| Item Description | Analytic value can include but is not limited to analysis of new or advanced technics, tactics, and procedures; new and novel malware; or if the destruction of this data would hinder ongoing or future operations. Anonymized information about the type of vulnerability when matched with critical infrastructure sector in aggregate can provide information to said sector on threat actor techniques and tactics.<br>Coast Guard CPTs conduct a variety of cyber missions to defend the MTS. The raw data is collected by the deployable mission support suite for analysis to determine impacts, such as potential vulnerabilities or malicious activity. Analytically relevant data is the portion of data collected that does contribute to analysis. To collect data, CPT analysts place sensors on the mission partners network that collects a mirror copy of the data transmitting through the network or through an end point agent that collects a copy of the host machine’s data. Once the data is collected, data is analyzed by CPT analysts and determined whether it is analytically relevant or not. Analytically relevant is further examined and used to form conclusions shared in the final technical report.<br>In the event that vulnerabilities or malicious activity are found during a CPT mission, the raw mission data of analytic value could be used for investigative purposes. Raw mission data is not shared. Raw data of analytic value is used to inform CPT mission planning. |

| | |
|---|---|
| | Raw data of analytic value is not created outside of CGCYBER. The Coast Guard currently has three CPTs. Each CPT collects approximately 10 TB of raw data per year for a total of 30 TB of data collected. The volume of raw data that is analytically relevant is highly variable from mission to mission. All members of the team that generated the raw data have access to the system, which is approximately 40 people. All 40 members contribute to the reports in some way when assigned. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 047-01-007, Revision # 03 |
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017 |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Temporary |
| Cutoff Instructions | Cut off at end of Calendar year. |
| Retention Period | Other: Destroy upon termination or fulfillment of contractual obligations with mission partners, but no later than 7 years after cutoff. |
| ADDITIONAL INFORMATION | |
| Are any of the records covered by this item national security classified? | No |
| GAO Approval Required | Requested and Received |

| DAA-0026-2022-0001-0003 | STATUS: Active |
|---|---|
| ITEM GENERAL INFORMATION | |
| Item Title | Story Boards |

| | |
|---|---|
| Item Description | The Coast Guard CPTs conduct a variety of cyber missions to defend the MTS. After the missions are complete, story boards are created to summarize the key points of the operation. The storyboards are provided by the CPT conducting the mission via email to CGCYBER leadership (CGCYBER's Commander, Deputy Commander, and Operations Officer). Story boards are meant to serve as a high-level summary of the mission. They are used by CGCYBER leadership to digest the key takeaways of CPT missions. These records are not distributed outside of CGCYBER. With the proper need-to-know, offices outside of CGCYBER could request redacted story boards. However, that is not standard practice and requests must be reviewed by the CGCYBER legal office prior to approval. Story boards generally do not inform planning. Story boards are only created by CGCYBER CPTs. They are not typically used outside of CGCYBER.<br>A story board is generated after each CPT mission. Each team typically conducts 12 missions per year. There are currently 3 CPTs, so an estimated 36 story boards will be generated each year.<br>All members of the teams that generated the report have access to the system on which story boards are maintained, which is approximately 40 people. All 40 members contribute to the out briefs in some way when assigned.<br>Drafts are created during the production of a story board. Drafts are necessary as the story board is routed through the chain of command prior to completion. This record is for the draft versions and the final copy of the story board. The story board is a standalone document. It is not encompassed into one case file with the other items in this schedule. As such, story boards generated after CPT missions are not considered part of a larger case file. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 047-01-007, Revision # 03 |
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017 |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |

| | |
|---|---|
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| **DISPOSITION INSTRUCTION** | |
| Final Disposition | Temporary |
| Cutoff Instructions | Cut off at end of Calendar year after completion of Cyber Protection Team (CPT) Mission. |
| Retention Period | Other: Retain no less than 90 days but no longer than one year. |
| **ADDITIONAL INFORMATION** | |
| Are any of the records covered by this item national security classified? | No |
| GAO Approval Required | Requested and Received |

| DAA-0026-2022-0001-0004 | STATUS: Active |
|---|---|
| **ITEM GENERAL INFORMATION** | |
| Item Title | Indicators of Compromise |
| Item Description | Coast Guard Cyber Command (CGCYBER) Cyber Protection Teams (CPTs) were established to offer cybersecurity capabilities to partners in the marine transportation system (MTS). CPT missions generate records related to indicators of compromise (IOCs) and data that is stored in supporting infrastructure. IOCs are reports that contain information regarding previously unknown indicators of potential information technology (IT) or operational technology (OT) system compromise in relation to a known cyber vulnerability. This generally includes an overview of the compromise that the indicators are associated with and technical details of what to look for when defending an IT and/or OT system. If IOCs are discovered and determined to be previously unknown a document detailing the IOC is drafted, usually with cybersecurity partners like the Cybersecurity and Infrastructure Security Agency (CISA). Upon draft completion and internal review for publication these records are widely shared via publicly available web interfaces. These records are meant for wide dissemination to share knowledge of cybersecurity vulnerabilities impacting the MTS. Mission partners are not identified in IOC publications. The Cybersecurity Information Sharing Act (CISA) of 2015 is a |

| | |
|---|---|
| | federal law designed to “improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.” CISA 2015 facilitates cyber information sharing of cyber threat indicators and defensive measures within the government and with non-federal entities. IOCs discovered during CPT missions are uniquely suitable for achieving CISA 2015’s information sharing goals because this data includes information and identifiers from private sector networks that may be compromised by malicious actors. Thus, it contains or may contain cyber threat indicators and/or cyber threat information. Once the information is shared, agencies/entities who gain access will be able to analyze the IOCs and protect their systems from compromise.<br>Normally, IOCs that are discovered on CPT missions are shared with government and non-federal entities and no further action takes place outside of CGCYBER. However, Cybersecurity Advisories are bulletins that describe IOCs discovered on CPT missions that other agencies have also observed. Cybersecurity Advisories are released in conjunction with partner agencies to the public.<br>IOCs are used to inform CPT mission planning. IOCs are only created by CGCYBER CPTs within the Coast Guard. IOCs are rarely released by the Coast Guard, approximately one per year is released. All members of CGCYBER CPTs and support personnel contribute to the records of IOCs discovered on CPT missions and have access to the records for their work. Drafts are created during the production of an IOC. Drafts are necessary as the IOC is routed through the chain of command prior to completion. This record is for the draft versions and the final copy of the IOC. The IOC is a standalone document. It is not encompassed into one case file with the other items in this schedule. As such, IOCs generated after CPT missions are not considered part of a larger case file.<br>When IOCs are used to generate Cybersecurity Advisories, they are maintained in a public CISA database. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 047-01-007, Revision # 03 |

| | |
|---|---|
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017 |
| **SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS** | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| **DISPOSITION INSTRUCTION** | |
| Final Disposition | Temporary |
| Cutoff Instructions | Cut off at end of Calendar year when Indicators of Compromise (IOC) is released and/or shared by USCG Cyber Command. |
| Retention Period | Destroy no later than seven year(s) after cutoff |
| **ADDITIONAL INFORMATION** | |
| Are any of the records covered by this item national security classified? | No |
| GAO Approval Required | Requested and Received |

| DAA-0026-2022-0001-0005 | STATUS: Active |
|---|---|
| **ITEM GENERAL INFORMATION** | |
| Item Title | Final Technical Reports |
| Item Description | The final technical report is the same as the technical report. It is designated as final upon legal and command clearance.<br>Coast Guard CPTs conduct a variety of cyber missions to defend the MTS. Technical reports are written by CPTs to memorialize the findings of these missions. There has been congressional interest in the CPTs' final technical reports. CGCYBER is regularly asked to provide briefings to congressional staffers and occasionally to congressional members on cyber threats to the Marine Transportation System. Previous congressional inquiries include an assessment of the vulnerability of maritime critical infrastructure and the potential impact of malicious cyber activity on MTS entities. CPT final technical reports are the primary source of information for those briefings.<br>The FY22 CPT final technical reports were provided to Office of Inspector General (OIG) auditors during the ongoing Audit of U. S. Coast Guard Cybersecurity Efforts to Protect the U.S. Supply Chain. |

These records fit at the conclusion of a CPT mission to memorialize findings. The final report is drafted after the mission by the mission element lead to encompass actions taken and impact during the mission. An example of actions taken that might be included in the technical report is an attack path, which consists of an initial access vector, how the team pivoted through the network to increase their privileges, and an explanation of the effects that could be delivered to the network through these actions. This report is routed through CGCYBER leadership before being released to the mission partner and local Captain of the Port. If requested by external entities CGCYBER Legal will determine if the entity is eligible to receive the record. If deemed eligible the requesting entity will receive a sanitized copy with no information attributable to the mission partner.
Following a mission, CPTs deliver the final technical report only to the mission partner, local captain of the port, and CGCYBER leadership. Outside of that hand off, there are no other offices that the final technical reports are delivered to automatically. With the proper need-to-know, offices outside of CGCYBER can request redacted final technical reports, however, that is not standard practice and requests must be reviewed by the CGCYBER legal office prior to approval.
Final technical reports are used to inform CPT mission planning. Final technical reports are also used to create Cyber Trends and Insights in the Marine Environment (CTIME) Reports (Item 0008).
Final technical reports are only created by CGCYBER CPTs.
A final technical report is generated after each CPT mission. Each team typically conducts 12 missions per year. There are currently three CPTs, so an estimated 36 final technical reports will be generated each year.
All members of the team that generated the final technical report have access to the system, which is approximately 40 people. All 40 members contribute to the reports in some way when assigned.

| | |
|---|---|
| | Drafts are created during the production of a final technical report. Drafts are necessary as the report is routed through the chain of command prior to completion. This record is for the draft versions and the final copy of the final technical report. The final technical report is a standalone document. It is not encompassed into one case file with the other items in this schedule. As such, final technical reports generated after CPT missions are not considered part of a larger case file. |
| Is this item media neutral? | Yes |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 047-01-007, Revision # 03 |
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017. |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Permanent |
| Cutoff Instructions | Cut off at end of Calendar year when report is released to Mission Partner. |
| Are there multiple instructions for this item? | No |
| Transfer Instruction | Transfer to the National Archives in 5 year blocks 15 year(s) after cutoff |
| ADDITIONAL INFORMATION | |
| Legal citation related to record retention (if applicable) | N/A |
| Current Records Format | Analog - Paper Records:40 Technical reports per year for a total of 160. Technical reports average between 40-70 pages |
| Approximate first year of records covered by this authority | 2021 |
| End year of records covered by this authority | Still being created |
| Date span of the initial transfer | From: 01/01/2021 To: 12/31/2025 |
| Frequency of transfer | 5 |

| | |
|---|---|
| Are any of the records covered by this item subject to a FOIA exemption? | Yes |
| FOIA Exemption(s) | FOIA (b)(3) Statute,<br>FOIA (b)(4) Trade Secrets and Commercial or Financial Information,<br>FOIA (b)(6) Personal Information |
| What is the related statute for the FOIA B(3) exemption? | The Cybersecurity Information Sharing Act of 2015, codified at 6 U.S.C. §§ 1501– 1510 |

| DAA-0026-2022-0001-0006 | STATUS: Active |
|---|---|
| ITEM GENERAL INFORMATION | |
| Item Title | Out Briefs |
| Item Description | Out briefs summarize the initial mission findings for the mission partner, the local Coast Guard captain of the port, and CGCYBER leadership. Out briefs are typically in PowerPoint format and contain information such as who was involved in the mission, what actions were taken, the impact of those actions, and recommendations based on the impact. For example, the out brief might describe how the CPT conducted a simulated phishing attack and were able to gain credentials and access to the mission partner’s database. A post mission recommendation in that example might be to conduct phishing training for the mission partner’s workforce.<br>There are no other offices that the out briefs are delivered to automatically. With the proper need-to-know, offices outside of CGCYBER can request redacted out briefs. However, that is not standard practice and requests must be reviewed by the CGCYBER legal office prior to approval.<br>Out briefs generally do not inform planning.<br>Out briefs are only created by CGCYBER CPTs. They are not typically used outside of CGCYBER. An out brief is generated after each CPT mission. Each team typically conducts 12 missions per year. There are currently three CPTs, so an estimated 36 out briefs will be generated each year. |

| | |
|---|---|
| | Drafts are created during the production of an out brief. Drafts are necessary as the out brief is routed through the chain of command prior to completion. This record is for the draft versions and the final copy of the out brief. The out brief is a standalone document. It is not encompassed into one case file with the other items in this schedule. As such, out briefs generated after CPT missions are not considered part of a larger case file. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 047-01-007, Revision # 03 |
| Manual Title | Department of Homeland Instruction Manual, Handbook for Safeguarding Sensitive Personally Identifiable Information (SPII), December 2017. |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Temporary |
| Cutoff Instructions | Cut off at end of Calendar year after out brief is released. |
| Retention Period | Other: Retain no less than 90 days but no longer than one year. |
| ADDITIONAL INFORMATION | |
| Are any of the records covered by this item national security classified? | No |
| GAO Approval Required | Requested and Received |

| DAA-0026-2022-0001-0007 | STATUS: Active |
|---|---|
| ITEM GENERAL INFORMATION | |
| Item Title | Cyber Trends and Insights in the Marine Environment (CTIME) Reports |

| | |
|---|---|
| Item Description | Annual publication that aggregates information regarding vulnerabilities observed by Cyber Protection Teams (CPT) in the field during cyber missions. Reports provide awareness in industry of common vulnerabilities. Reports are created by Coast Guard Cyber Command Cyber Protection and Effects Division with contributions from all of the CPTs. The report summarizes the trends observed throughout the year's CPT missions as well as a summary of the information contained within the final technical reports (Item 0005). However, more than just final technical reports are used to create the CTIME. This report is anonymized to ensure mission partners' identities are not revealed. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 026 |
| Manual Title | Cyber Trends and Insights in the Marine Environment (CTIME) Reports |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Permanent |
| Cutoff Instructions | Cut off at end of Calendar year when Cyber Trends and Insights in the Marine Environment (CTIME) Report is released. |
| Are there multiple instructions for this item? | No |
| Transfer Instruction | Transfer to the National Archives in 5 year blocks 15 year(s) after cutoff |
| ADDITIONAL INFORMATION | |
| Current Records Format | Textual data:39 MB |
| Approximate first year of records covered by this authority | 2021 |
| End year of records covered by this authority | Still being created |
| Frequency of transfer | 5 |

| | |
|---|---|
| Are any of the records covered by this item subject to a FOIA exemption? | No |

| | |
|---|---|
| Group Title | Maritime Cyber Communications |
| Group Description | Maritime Cyber Communications are created by CGCYBER for the purpose of highlighting cybersecurity items of interest such as malicious cyber actors and activity, newly identified vulnerabilities, and other items deemed appropriate to release to the Marine Transportation System (MTS). Within this broad umbrella, there are three categories of communications: Maritime Advisories, Maritime Cyber Alerts (MCA), and Maritime Cyber Bulletins (MCB). The Maritime Cyber Advisories are reports generated by other federal agencies (CISA, FBI, NSA). CGCYBER publishes these advisories to highlight their relevance to the MTS. CGCYBER does not create or own these advisories, CGCYBER just “reposts” them." |
| DAA-0026-2022-0001-0008 | STATUS: Active |
| ITEM GENERAL INFORMATION | |
| Item Title | Maritime Cyber Alerts (MCA) |
| Item Description | A security notification detailing a specific cybersecurity threat, risk, incident or vulnerability, that if not addressed, could place MTS critical infrastructure at risk. The MCA includes sanitized details of the incident and/or vulnerabilities, tactics of threat actors, indicators of compromise (IOC), and mitigation strategies. All MCAs can be found at: Coast Guard Maritime Industry Cybersecurity Resource Website |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 026 |
| Manual Title | Maritime Cyber Alerts (MCA) |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Permanent |

| | |
|---|---|
| Cutoff Instructions | Cut off at end of Calendar year when Maritime Cyber Alert (MCA) is released. |
| Are there multiple instructions for this item? | No |
| Transfer Instruction | Transfer to the National Archives in 5 year blocks 15 year(s) after cutoff |
| ADDITIONAL INFORMATION | |
| Current Records Format | Born Digital - Web Records:2 MB |
| Approximate first year of records covered by this authority | 2023 |
| End year of records covered by this authority | Still being created |
| Are any of the records covered by this item subject to a FOIA exemption? | No |
| DAA-0026-2022-0001-0009 | STATUS: Active |
| ITEM GENERAL INFORMATION | |
| Item Title | Maritime Cyber Bulletins (MCB) |
| Item Description | A security notification similar to a Maritime Cyber Alert (MCA), but for which it has been determined that the information is less technical, or for which there are not mitigation strategies available to share. MCBs may contain cyber threat information that is not directly related to the Marine Transportation System (MTS) but could have second or third order effects that could impact the MTS and maritime critical infrastructure. All MCBs can be found at: Coast Guard Maritime Industry Cybersecurity Resource Website. |
| Is this item media neutral? | No |
| Media limitation | Digital only |
| Is this item a Big Bucket? | No |
| MANUAL CITATION | |
| Agency Code | 026 |
| Manual Title | Maritime Cyber Bulletins (MCB) |
| SUPERSEDED AGENCY DISPOSITION AUTHORITIES AND GRS DEVIATIONS | |
| Does this item supersede existing disposition authorities? | No |
| Is this item a deviation from the GRS? | No |
| DISPOSITION INSTRUCTION | |
| Final Disposition | Permanent |

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

| | |
|---|---|
| Cutoff Instructions | Cut off at end of Calendar year when Maritime Cyber Bulletin (MCB) is released. |
| Are there multiple instructions for this item? | No |
| Transfer Instruction | Transfer to the National Archives in 5 year blocks 15 year(s) after cutoff |
| ADDITIONAL INFORMATION | |
| Current Records Format | Born Digital - Textual Data:2MB |
| Approximate first year of records covered by this authority | 2020 |
| End year of records covered by this authority | Still being created |
| Are any of the records covered by this item subject to a FOIA exemption? | No |

Records Schedule Number: DAA-0026-2022-0001

Status: APPROVED
Date Approved: 07/15/2026

## Signatory Information

| Action | User | Date |
|---|---|---|
| Approve | Edward Forst (Acting Archivist) | 07/15/2026 |

This schedule was signed outside of the ERA system using Standard Form 115.

NARA staff updated ERA to reflect this approval, moving the record schedule into an approved status. The approved status allows for generation of a PDF indicating that the schedule has been approved, and allows an agency to use the schedule in ERA to create transfer requests. The approved date in the system and on the PDF version of the records schedule reflects the system actions.