USCG Office of Maritime Cybersecurity Policy (CG-MCP)
Mission Management

Category	Administrative				
Title	DoD SAFE Instructions for Cybersecurity Plan, Cybersecurity Assessment, Waiver & Equivalency Request Submissions				
Serial	MCP-WI-003	Orig. Date	03June26	Rev. Date	N/A
Disclaimer:	This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to, nor does it impose legally-binding requirements on any party. It represents the Coast Guard's current process for secure transmission of Cybersecurity Plans (CSP), Cybersecurity Assessments (CSA), and waiver and equivalence requests.				
References:	(a) 33 CFR Part 101, Subpart F – Cybersecurity (b) 49 CFR Part 1520 – Protection of Sensitive Security Information				

A. Purpose. This work instruction provides guidance regarding the Coast Guard's process for secure transmission of CSAs, CSPs, waivers and equivalency requests using the DoD SAFE portal. The required security documents are considered Sensitive Security Information (SSI) and must be handled and transmitted as such. This instruction establishes a uniform method for submission of SSI documents for the purpose of complying with ref (a) and (b).

B. Action. The Coast Guard will use this instruction to guide the submission of CSAs, CSPs, waiver and equivalency requests under 33 CFR Part 101, Subpart F – Cybersecurity.

C. Background. 33 CFR Part 101, Subpart F – Cybersecurity became effective on July 16, 2025. This subpart set minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities to safeguard the security and resilience of the Marine Transportation System (MTS). Per reference (a), an owner or operator of U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR parts 104, 105, and 106 must ensure a CSP is developed, approved, and maintained. Additionally, per reference (a), an owner or operator may seek a waiver or an equivalency determination for the requirements in 33 CFR Part 101, Subpart F.

D. Discussion.

1. Process Flow for Submitting CSA, CSP, Waiver, or Equivalency Requests via DoD SAFE
   a. **Save Document:** Save an electronic copy of the CSA, CSP and other relevant documents to be uploaded as a PDF and encrypt the document(s) with a password.
   b. **Drop-Off Request:** The entity must submit a Drop Off request to the Coast Guard by emailing **CyberPlanReview@uscg.mil** or alternately, by contacting their local COTP representative.
   c. **Auto-Generated Email:** Once the Coast Guard initiates a drop off request, requestor will receive an auto-generated email containing a Request Code to the DOD SAFE webpage that

will allow for upload of the documents as a guest user. A drop-off request is only valid for 14 days.

i. To use DoD SAFE without a PIV/CAC, non-DoD users can log in as a "guest" by clicking "Cancel" when prompted for a certificate.

ii. If the webpage link contains text prior to the https:// that prevents the link from being active, copy and paste the link into a browser address bar and remove the text prior to the https:// for the weblink to be usable.

d. **Request Code:** Use the Request Code to access the submission page.

e. **Webpage Access:** If the guest user uses the webpage link within the provided auto-generated email, the DoD SAFE webpage will open containing the sender's email address auto-populated.

f. **Short Note:** Fill out the short note to the recipients.

g. **File Upload:** Upload the files using "Click to Add Files" or "Drag Them Here" option. Each file upload offers an optional description. This can be used to identify the files uploaded as described in the short note.

h. **Drop-off Confirmation:** Click on Drop-off Files. Click "OK" on the pop-up message confirming the upload does NOT contain classified information (this is not referencing Sensitive Security Information). A confirmation webpage will indicate if the Drop-Off was completed.

i. Send the encryption password to the Coast Guard (same address used to request the drop off) in a separate email using the applicable contact information from paragraph D.1.(c).

i. **Recipient Notification:** The Coast Guard will receive an email containing a link to pick up the files. The email will contain a claim passcode and full information about the drop-off including the sender information, the file name and descriptions, as well as any notes.

Note: Problems accessing the DoD SAFE site by external (non-PIV card) users are typically due to SSL and/or client certificate issues. If the user receives a warning about a problem with the website's security certificate, this is because their browser is not configured to trust the DoD certificate authorities. The user can accept the risk and click on the option to continue to the website.

E. Additional Information. Questions or concerns regarding this document should be directed to the CG-MCP at MTSCyberRule@uscg.mil.

C.N. Parham

PARHAM.CHARLES.NICHOLAS.1250657656

Digitally signed by PARHAM.CHARLES.NICHOLAS.1250657656
Date: 2026.06.04 10:37:32 -04'00'

C. N. PARHAM
Chief, Office of Maritime Cybersecurity Policy
By direction