WEB ACCESS WAVIER FOR INTERNAL USERS

Use this form to request access from internal systems to external Websites

Users requesting access from internal (Garrison: NMCI and Legacy) systems behind USMC protected network boundaries to external websites will use this form. Users must complete sections A-E and submit to the local IAM via digitally signed email. Instructions are attached.

Section A. Requester Contact Information

Last Name	***First Name***	***MI***	***Rank***	***Phone Number***

Unit	***Installation***	***Email Address***

Section B. Client Information

Hostname	***IP Address***

Section C. Requested Website Information

Website *(URL)*	
Official System or Application Name	
Last Day Required *(MM/DD/YY)*	☐ **Indefinite**

Error Message

Section D. Justification

Section E. Mission Impact, If Denied

Section F. Local Validation (IAM /G-6 Only)	
Local Information Assurance Manager/G-6	***Recommend Waiver?*** ☐ **YES – Forward to regional IAM via digitally signed email** ☐ **NO - Return to requester**
Section G. Regional Validation (TOP 16 Commands, IAW NETOP Reporting Structure)	
Regional Information Assurance Manager	***Recommend Waiver?*** ☐ **YES - Forward to MCNOSC Service Desk via digitally signed email** ☐ **NO - Return to requesting IAM**
Section H. MARCERT Risk Analysis / Recommendation (MARCERT only)	
Analyst Name	***Recommend Waiver*** ☐ **YES – Forward to MCNOSC Watch Officer** ☐ **NO – Forward to MCNOSC Watch Officer**
Section I. MCNOSC Approval / Disapproval (MCNOSC Watch Officer only)	
☐ **Approve access from NMCI USMC COI** ☐ **Approve access from USMC Legacy Network** ☐ **Approve access from USMC Deployed Network** ***Approving Authority***	***Approve Waiver*** ☐ **YES – Modify MCEN to facilitate request** ☐ **NO – High CND risk, return to sender** ***Recommend Waiver*** ☐ **YES – Low CND risk and no policy violation** ☐ **NO – MCEN policy violation, forward to MCEN DAA**
Section J. DAA Approval / Disapproval	
Approving Authority	***Approve Waiver*** ☐ **YES** ☐ **NO** ***Approve for Commercial ISP*** ☐ **YES** ☐ **NO**

Section A. Requester Contact Information

This section of the form is to be completed by the individual Marine or Unit requesting.

1) Input the requestor's base, post, or station in the "Installation" field.

Section B. Client Information

This section is used to identify where the requester is attempting to access the external website from..

Hostname – Can be found by typing 'hostname' from a command prompt

IP Address – Can be found by typing 'ipconfig' from a command prompt.

Section C. Website Exclusion Information

This section is for MCEN Users to request a waiver for access to a specific web site, category or Top Level Domain (TLD) which has been blocked due to the increased scope of Computer Network Defense Initiatives or Information Assurance Policies..

URL – This block must contain the exact URL of the website the waiver applies to. For example, https://www.usbank.com, note the "s" in https, for a SSL secured website, or http://www.cnn.com for a non-secure website.

Official System or Application Name – This is the official government or commercial name of the system, or application. For example, the Defense Travel System (DTS) is a web based portal..

Error Message – This field will include the exact text of the error message currently being displayed when attempting to use the application or connecting to the remote system.

Last Day Required – This field must contain the last day access to the website is required. This field will be used when access to the website is only required for a specific amount of time. The format for this field is MM/DD/YY. If access to the website will be required indefinitely then check indefinite and leave the field blank. Waivers my be denied based on length of request. Validate timeline requirements.

Section D. Justification

Explain the specific operational reasons the website is required. Explain the function of the system or application being used.

Section E. Mission Impact if Denied

Explain how the mission of the organization or specific job function will be impacted if waiver or exclusion request is disapproved.

Section F. Local Validation (IAM /G-6 Only)

Local IAMs will coordinate with local users and Commands to confirm validity of requests and determine if the access issue was related to a network outage. Access issues due to a network outage will not require a web access waiver.

Section G. Regional Validation (TOP 16 Commands, IAW NETOP Reporting Structure)

G-6(s)/IAM(s) of the top 16 Commands will review and validate the local web access requests prior to submission to the MCNOSC via digitally signed email. Send emails to the MCNOSC at commandcenter@mcnosc.usmc.mil with the following subject line format: **Web Access Request [Insert Name of Top 16 Command].**

Section H. MARCERT Risk Analysis/Recommendation

For MARCERT use only.

Section I. MCNOSC Approval/Disapproval

For MCNOSC use only.

Section J. USMC DAA Approval / Disapproval

For USMC DAA use only.

Request Routing Process

To request a website waiver the following process must be followed.

1) Requestor completes sections A-F and forwards request via digitally signed e-mail to their local Information Assurance Manager (IAM). If requestor is already using assets that are external to the MCEN, then the user must coordinate with their local G-6/IAM for completion of all required waiver information fields.

2) The local IAM validates the justification for the request and forwards the valid request via digitally signed e-mail to the appropriate major command IAM. If the request is not valid it is returned to the requester by the local IAM.

3) The major command IAM validates the request for violations of command IA policies and forwards the valid request via digitally signed e-mail to MCNOSC Command Center at commandcenter@mcnosc.usmc.mil. If the request is not valid the major command IAM forwards the request back to the local IAM.

4) The MCNOSC processes the request and forwards it back to the major command IAM, local IAM, and requestor via encrypted e-mail.

   If a website request is not approved by the MCNOSC, the major command may request that MCNOSC forward the waiver request up to the Information Assurance Division of the Marine Corps' C4 Department for final review. If the request is subsequently denied by the C4 DAA, the MCNOSC will notify the major command IAM, local IAM, and requestor via a digitally signed e-mail.