

**FOR OFFICIAL USE ONLY**

**WEB ACCESS WAIVER FOR INTERNAL USERS**

*Use this form to request access from internal systems to external Websites excluding .MIL and .GOV*

Use this form to request access from internal MCEN systems (behind USMC protected network boundaries) to external websites, not including .MIL or .GOV sites. Users complete sections A-E then submit to the local ISSM via digitally signed email. Instructions attached. Do not use this form for problems accessing .MIL or .GOV; submit a Request for Modification/Troubleshooting via Remedy ticket.

**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**

--

**FOR OFFICIAL USE ONLY**

**WEB ACCESS WAIVER FOR INTERNAL USERS**

*continued*

**Section F. Local Validation: G-6 /ISSM only (ISSM was previously titled IAM)**

<i>Local G6 / Information System Support Manager</i>	Recommend Waiver
	<p style="text-align: center;">YES – Forward to regional ISSM via digitally-signed email</p> <p style="text-align: center;">NO – Return to Requester</p>

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

<i>Regional Information System Support Manager</i>	Recommend Waiver
	<p style="text-align: center;">YES – Forward to MCNOSC Service Desk via digitally signed email</p> <p style="text-align: center;">NO – Return to Requesting ISSM</p>

**Section H. DCOS Risk Analysis / Recommendation (DCOS only)**

<i>DCOS Analyst Name</i>	Recommend Waiver
	<p style="text-align: center;">YES – Forward to MCNOSC Watch Officer</p> <p style="text-align: center;">NO – Forward to MCNOSC Watch Officer</p>

**Section I. MCNOSC Approval / Disapproval (MCNOSC Watch Officer only)**

<b>Approve access from MCEN</b>	
<b>Approve access from USMC Deployed Network</b>	
<b>Approving Authority</b>	<b>Approve Waiver</b>
	<p style="text-align: center;">YES – Modify MCEN to facilitate request</p> <p style="text-align: center;">NO – HIGH CND RISK: Forward to C4 AO</p>

**Section J. C4 AO Approval / Disapproval**

<b>Approving Authority</b>	<b>Approve Waiver</b>	<b>YES</b>	<b>NO</b>
	<b>Approve for Commercial ISP</b>	<b>YES</b>	<b>NO</b>

**INSTRUCTIONS TO COMPLETE WEB ACCESS WAIVER**

**Routing Process for the Request:** The Access Waiver Request must be processed in this order.

1. Requestor completes sections A-E and forwards request via digitally signed email to their local Information System Support Manager (ISSM), previously titled 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/ISSM for completion of all required waiver information fields.
2. The local ISSM validates the justification for the request and forwards the valid request via digitally signed email to the appropriate major command ISSM. If the request is not valid it is returned to the requester by the local ISSM.
3. The major command ISSM validates the request for violations of command IA policies.  
Valid requests are forwarded via digitally signed email to MCNOSC at [operationscenter@mcnosc.usmc.mil](mailto:operationscenter@mcnosc.usmc.mil).  
If the request is not valid the major command ISSM returns the request to the local ISSM.
4. The MCNOSC processes the request and returns it to the major command ISSM, local ISSM, and requestor via digitally signed e-mail.
5. 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.
6. If the request is subsequently denied by the C4 AO, the MCNOSC will notify the major command ISSM, local ISSM, and requestor via a digitally signed email.

**Section A. Requester Contact Information**

This section of the form is completed by the individual Marine or Unit requesting.  
Input the requestor's base, post, or station in the "Installation" field.

**Section B. Client Information**

From where is the requester/user trying to access the external website? Identify the machine location by:  
**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** – Must provide the *exact* URL of the website the waiver applies to. For example - <http://www.cnn.com> for a non-secure website or <https://www.usbank.com> for an SSL secured website which has the "s" in https.  
**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** – Include the *exact* text of the error message that displays 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. Use this field only when access to the website is 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 date field blank.  
Waivers may be denied based on length of request; validate the 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 G-6 /ISSM only (ISSM was previously titled IAM.)**

Local ISSMs 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)/ISSM(s) of the top 16 Commands will review and validate the local web access requests prior to submission to the MCNOSC. Send via digitally signed email. Email to the MCNOSC at [operationscenter@mcnosc.usmc.mil](mailto:operationscenter@mcnosc.usmc.mil).  
Use the following subject line format: **Web Access Request [Insert Name of Top 16 Command]**.

**Section H. DCOS Risk Analysis/Recommendation**

For DCOS use only.

**Section I. MCNOSC Approval / Disapproval**

For MCNOSC use only.

**Section J. C4 Authorizing Official (AO) Approval / Disapproval**

For C4 Authorizing Official (AO) use only. (AO was previously titled DAA.)