Equipment Entry Authorization (EEA) Form

This form is required to hand carry Non AUTEC Computers and Communication / Audiovisual equipment, (Cameras, Video Recorders, Recording Devices, radio transmitters, etc.), into AUTEC operational areas. **Current policy prohibits NMCI & Non-Government Legacy computers from being connected to the AUTECNet. Requests for AUTECNet accounts require the completion of a SAAR-N (OPVNAV 5239/14) form. Please forward completed forms to: EEA@autec.navy.mil**

Individual Requiring Authorization: **Last Name**: **First:** **Middle Initial:**

Citizenship: ☐ **US** ☐ **Other ---** If Other What Nationality

SSN: Not Required at this time Agency:

Duration of Request – From: To:

AUTEC Sponsor : Dept: Phone Ext:

Highest Classification of Data Processed: Will Data be Retained by User : ☐ No ☐ Yes

** For the following 4 lines please use the **"Justification"** section to explain the use of the equipment **

Will Equipment be Connected to any AUTEC Classified Systems ☐ No ☐ Yes : **Identify Below ***

Will Equipment be connected to any AUTEC Unclassified Systems for a purpose other than access to the internet ☐ No ☐ Yes

Unclassified Network Services Required: ☐ None ☐ Internet via / ☐ AUTECNet)

☐ AUTECNet Domain services – Please indicate below what domain resources are required (other than the internet).

* Justification :

AREA REQUIRING ENTRY (CHECK ALL THAT APPLY)

☐ CCB ☐ Range SS ☐ HQ WPB ☐ Other Building(s) (Specify) :

Bldg Room No(s):

Specify Area Names:

EQUIPMENT & ATTRIBUTES

Equipment Property Control Number:

ITEM	MANUFACTURE	MODEL NO.	SERIAL NO.	Operating Sys

Is this equipment owned by a DON agency ☐ No ☐ Yes MAC address required for AUTECNet access:

Is this equipment NMCI issued: ☐ Yes ☐ No --- NMCI issued computers are currently prohibited from connecting to the AUTECNet.

Is Anti Virus Software installed ☐ N/A ☐ No ☐ Yes --- If, Yes Specify type:

Please check all applicable attributes: ☐ None (☐ Wireless capability ☐ Embedded Camera ☐ Infrared Port) - (☐ Writable CD ☐ Floppy Drive ☐ Removable Storage device ☐ Embedded Hard Drive ☐ Internal Microphone)

Network Security Officer: **(required only for non-stand alone equipment)** Date:

NUWCDETAUTEC IAM or authorized representative: Date:

SPONSOR RESPONSIBILITIES

The sponsor agrees that he/she is responsible for ensuring that the above authorized individual is briefed regarding the usage of equipment while at AUTEC and within assigned areas and all equipment and information will be operated / handled in accordance with AUTEC policies and or applicable DoN Information Assurance Program policies and procedures.

Sponsors are responsible for insuring that all applicable information is entered on the form before the form is forwarded. All items should have an entry, if not applicable enter N/A.

Please forward completed forms to EEA@autec.navy.mil **this is listed in the Global Directory as "Dist: Equipment Entry Authorization".**

1. Authorization is required for equipment entry into all AUTEC operational areas. If entry is authorized, the System Information Assurance Officer (IAO) or System Administrator (SA) for their respective system will provide the required briefing and determine the requirement for escort within the area

2. Assuring that visitors receive the required user briefings relative to the use of the authorized equipment within a specific controlled area is the responsibility of the Sponsor and must comply with AUTEC and or DoN IA security policies and procedures. **If assistance is required in the performance of said policies or with any briefing, the sponsor should contact Industrial Security ASD at (6370) or (6602) and in WPB (7437) or NUWCDETAUTEC Security WPB at (7332 / 7279) or ASD (5157).**

3. Users requiring access / connection to any AUTEC System will be based on equipment compliance and operational requirements and may be required to submit a **Systems Authorization Access Request Navy** form (SAAR-N/OPNAV 5239/14). All EEA forms shall be forwarded to Industrial Security.

Please Note: Currently Non DoN and NMCI issued computers are prohibited from connecting to the AUTECNET.

4. Equipment will NOT BE CONNECTED to any AUTEC system without specific authorization from the Network Security Officer and the cognizant IAO or SA.

5. Equipment will only be operated in areas specified on the Equipment Authorization Form.

6. Users not authorized access to the AUTECNet may access the Internet via the RECNET. Sponsors are responsible for making the necessary arrangements.

7. All classified hard copy and/or media resulting from use of the authorized equipment will be the responsibility of the individual requesting authorization (sponsor). Appropriate marking and/or transmittal of all classified material may be requested of Document Control through the Sponsor.

8. Where applicable, all computers to be connected to any AUTEC systems will be scanned to insure they are free of any malicious code and that their anti virus signature files are up to date. Sponsors should make arrangements with Hardware engineering to install A/V software and update signature files if necessary.

9. If visitors are to hand carry classified material they must have prior courier authorization from their respective command/agency. All classified material to leave the AUTEC project must be processed through Document Control.

10. Government computer systems are for official use only. However, under certain conditions, personal use of E-mail and the Internet, subject to specific restrictions in accordance with NAVSEAINST 2300.1, is permitted. Publicly accessible web pages may not be established without official authorization. These restrictions also apply to privately owned computers routed through government network services.

a. Individuals who access government communication systems, whether from the office or from home, do so with the understanding that such use is not secure or anonymous**. Use of any government computer resource constitutes an express consent to monitoring at all times.** Monitoring will include surveys of individual Internet and World Wide Web site access activities.

b. Access privileges may be revoked for any perceived misuse. Any abuse may be the basis for disciplinary action on the part of the command including criminal prosecution.

c. In the workplace, personal communications and Internet access should be limited to authorized break periods or before or after duty hours. Outside the work place, access is restricted to times outside of normal operational periods, which extend from 0730-1630, Monday through Friday.

d. Within the office environment, personal communications should be kept infrequent and short. Outside the office, communications should be kept to a reasonable period so that they do not overburden or affect the performance of the communications network.

f. The Government must not incur any direct long distance charges or other fees for these communications.

g. Authorized access does not extend to the following: (1) Communications that solicit charitable, business, or advertising contributions; (2) Communications that engage in other commercial activities in support of an organization, private business enterprise, or any other use that may reflect adversely on the DoN or which is incompatible with public services (e.g., threatening or harassing messages, hate sites, transmission or receipt of pornographic or other sexually explicit materials or communications); and (3) Any other use that violates statutes or regulations or is used to gain unauthorized or unlawful access to information.

11. All incidents where a known compromise or a suspected compromise of classified information has occurred must be reported to the AUTEC sponsor immediately. Additionally all incidents where the integrity of the unclassified network may have been compromised must also be reported.