



GFE-VPN Access Request Form



Purpose:

This form is used to request access for systems through the NNMC firewalls. The Information Security Team will evaluate information contained in this form and access will be granted based on need. This evaluation process takes up to **one business week** to determine if there are any security risks and to obtain the necessary authorization to complete this request.

Instructions:

1. Collect all the information contained on page 2 and 3 of this form. Contacts, purpose, justification, and technical details. Directorate signature is required for VPN Account Setup as well as the distribution of G.F.E. (Government Furnished Equipment) Laptops. **This information must be filled out accurately and completely to satisfy documentation requirements.**
2. You must forward this request to your Government representative WITHOUT IP address information if you are using insecure communication methods. It is against NNMC policy to send IP address information unencrypted electronically or otherwise in insecure communications channels. Have your Government representative submit this form using **secured email** to thomas.rauch@med.navy.mil. THIS EMAIL MUST BE SIGNED USING A VALID DoD PKI CERTIFICATE. The DoD PKI certificate will be used to authenticate your request. Please update the file name to reflect the user's name, ie: '**Doe_Jim-VPN-Request-Form.doc**'.
3. If you have any questions, please contact the NNMC ISSM at (301-295-5467) or the INFOSEC Team at (301-319-4270).

For Office Use Only

| | |
|-------------------------------|--|
| Received by: | |
| Date: | |
| Approved? YES NO | |
| If NO Reason for disapproval: | |
| | |

Part A – Directorate Authorization Contact Information

Directorate contact information and signature. This information should be for your Directorate contact information who is authorizing your VPN account.

| | | |
|------------------------|--------------|---------------|
| Name (First, MI, Last) | Rank | Email Address |
| Office Phone | Directorate: | |
| Command | Building | Room |
| Signature | | |

Local (requester) security contact information. This should be your company's security officer or immediate supervisor's information.

| | | |
|------------------------|------------------------|------------|
| Name (First, MI, Last) | Office Phone | Home Phone |
| Email Address | Secondary phone number | |

Requestor/User Contact Information

| | | |
|---------------------|-------------------|---------------|
| First Name, MI | Last Name | Rank |
| Office Phone Number | Home Phone Number | Email Address |

Part B – Justification

Please explain why you require VPN access to the NNMC network.

| |
|--|
| |
|--|

Describe the nature of business this system is involved in. Please provide a paragraph or two describing what the system does for your organization and what business your organization does.

| |
|--|
| |
|--|

Part C – Technical Details

Please provide the IP Address, MAC Address and Computer Name of your NNMC PC. You can find this information at a DOS command prompt `ipconfig /all`, on your NNMC PC.

| | | |
|------------|-------------|---------------|
| IP Address | MAC Address | Computer Name |
|------------|-------------|---------------|

Part D – GFE Laptop Details

Please provide the Mfg/Model and MAC Address of your GFE Laptop.

| | |
|-----------|-------------|
| Mfg/Model | MAC Address |
|-----------|-------------|

Navy Enterprise Information Technology (IT) Remote User Acknowledgement Form

This form will be retained by the command IAM for 12 months after Requestor's departure from the command.

| | |
|--|---------------------------------------|
| ACKNOWLEDGEMENT <i>(To be completed by Requestor)</i> | |
| NAME <i>(Last, First, Middle Initial)</i> | |
| ORGANIZATION | JOB TITLE & GRADE/RANK |
| TELEPHONE NUMBER | DEPT/DIVISION/CODE |
| CITIZENSHIP | |
| Immediate Supervisor | Immediate Supervisor Telephone Number |

Authority: Executive Order 10450, 9397; Public Law 99-474; the Computer Fraud and Abuse Act; 5 U.S.C Statute 301; 10 U.S.C. Part II; 14 U.S.C. Chapter 11; UCMJ; DOD 5500.7R, Joint Ethics Regulation; CJCSM 6510.01, DODD 8500.1 and SECNAVINST 5239.3A, DON Information Assurance (IA) policy.

1. Purpose: This user acknowledgement form outlines the terms, conditions and proper use for operating, accessing, managing, and/or using United States Navy Enterprise Information Technology (IT) resources remotely from a non DoD computer. All persons with access to Navy IT resources, whether authorized or not, are reminded that use of these resources is subject to monitoring.

2. Scope: Unless otherwise specified, this user acknowledgement applies to U.S. Armed Forces Uniformed Military members, U.S. Civil Service civilian employees, Department of Defense contractors, and Non-U.S. personnel (foreign military personnel, foreign civilian employees, or local nationals in host country), with access to USN provided or funded IT. This user acknowledgement applies to collateral Navy IT resources only.

3. Consent to monitoring: I am aware that by using Navy IT resources, I am subject to authorized monitoring for all lawful purposes and hereby consent to such activities. Furthermore, I am aware that there is *NO* right of privacy in this system. By my signature, I expressly consent to such monitoring and acknowledge that all information stored on or transmitted on Navy IT resources is subject to search and seizure, including searches or seizures initiated by law enforcement personnel, without the need of a search warrant or other search authorization.

4. Acknowledgement of Responsibilities:

- While remotely connected I am aware that Navy IT resources are for official use and authorized purposes related to assigned duties, which do not interfere or conflict with those assigned duties and do not violate law, regulation, or standards of conduct. Examples of violations include, but are not limited to use for commercial purposes or solicitations, hate speech, viewing pornography or sexually oriented adult material, or other unsolicited and prohibited communications, etc.
- I am aware authorized purposes may include limited personal use when permitted by Commanding Officers (also known as Local IA authority), within the limitations set forth in DoD 5500.7R, Joint Ethics Regulation. When permitted, I understand my personal use of Navy IT resources is still subject to monitoring as outlined in paragraph 3 above.
- I am aware I have the responsibility to safeguard Navy IT resources and the information

contained on them from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

- I am aware I will be limited to accessing only that data and software for which I am authorized and have a need-to-know.
- I am responsible for controlling access and determining the correct classification of any data I create, modify, or access and will ensure proper marking IAW SECNAV 5510.36. Furthermore, I am aware that I am responsible for ensuring such data is protected in accordance with the laws of the U.S. and/or any host country laws specified under U.S. and host country bi-lateral agreements or Status of Forces Agreement, where applicable.
- I will utilize only DoD-approved PKI for encryption and/or signing of data and/or email.
- I will digitally sign all official unclassified email and encrypt all sensitive email IAW DoDD 8500.1 (including but not limited to Privacy Act, For Official Use Only, and Operational Security (OPSEC) data).
- I will protect passwords and/or tokens commensurate with the level of information processed on the system, and not disclose them to any persons.
- I will construct strong passwords IAW DoD Instruction 8500.2, CJCSM 6510.01 and as outlined in current IA mandated training. I understand personal password sharing and embedded passwords (e.g. Windows password auto-save) are prohibited.
 - I will properly log off upon completion or departure from any Navy IT resource. If departing the area only briefly, I will screen lock the device or system.
- I will immediately report any security violations, electronic spillages or inappropriate activities to my Security Manager, Information Assurance Manager (IAM) or Local IA authority.
- I will adhere to all policies for the correct labeling and handling of media and storage devices.
- I will notify my IAM when I no longer have a need to access Navy IT resources (e.g. transfer, discharge, etc.).
- I will maintain a U.S. Government security clearance commensurate with the level of access I am granted.
- I will complete required user training annually and as directed.
- I am aware that I am being provided Government provided PKI software for use on my home PC. I will be responsible for the loading and maintenance of this software and will not expect ITD assistance in loading or maintenance of this software or the associated PKI Computer Access Card (CAC) reader.
- I am fully aware that the Department of the Navy and National Naval Medical Center Bethesda are not responsible for any damages, problems or required repair that may arise from loading the PKI software or installing the associated CAC reader.
- I will not print, download or transfer in any unapproved manner, sensitive data, (i.e. Protected Healthcare Information), I access while attached remotely to the NNMC Bethesda network.
- While attached remotely I will abide by the same rules and regulations that are associated with the hands on use of my computer at NNMC Bethesda.

Requestor's initials _____

Circle One: Military Civilian Contractor

5. Enforcement: Violation of the rules outlined above could result in loss of Navy IT resource privileges. Administrative, disciplinary, and/or criminal action pursuant to U.S. federal law, the Uniform Code of Military Justice, Navy regulations, and any host country laws specified under U.S. and host country bilateral agreements or Status of Forces Agreement may be taken.

FAX Back to NNMC Information Security at 301-295-6669

Signature:

Date: