SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

Executive Order 10450, 9397; Public Law 99-474, the Computer Fraud and Abuse Act. To record names, signatures, Department of Defense (DOD) ID Numbers, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense Systems and information. Disclosure of this information is voluntary; However, failure to provide the requested information may impede, delay, or prevent further processing of the request.

PART 1 (To be completed by Requestor)

1. Name (Last, First, Middle Initial)		2. Grade/Rank/Rate
3 Command	4. Depaartment/Division	5. Phone (Commercial or DSN)
6 Unclassified Email Address	7. DODD ID Number	8. PRD (YYYY-MM-DD)

9. Annual IC Cyber Awareness Training Requirement. (Must be completed for the current Fiscal Year)

☐ I acknowledge that a valid IC Cyber Awareness Certificate must be completed and submitted in order tomaintain network access.

10. USS Blue Ridge Domain User Security Statement (Enclosure 1 Included in this Package)

☐ I have read and will comply with the USS BLUE RIDGE Domain User Security Statement.

11. User's Signature	12. Date (YYYY-MM-DD)

PART 2 (To be completed by Supervisor or Government Sponsor)

13. Verification of Need to Know I certify that this user requires access as requested. ☐	14.Supervisor's Organization/Department

15. Supervisor's Phone Number	16. Supervisor's Email Address	17. Date (YYYY-MM-DD)
18. Supervisor's Name (Last, First, Middle Initial)	19. Supervisor's (Signature)	

PART 3 (To be completed by SSO or SSR)

20.Clearance Level (Including All Tickets) ☐ SI ☐ TK ☐ HCS ☐ G	21. Date of Investigation (YYYY-MM-DD)	22. Investigation Status ☐ Interim ☐ Final

23.SSO/SSR Phone Number	24. SSO/SSR Email Address	25. Date (YYYY-MM-DD)
26. Verified By (Last, First, Middle Initial)	27. Verified By (Signature)	

PART 4 (To be completed by BLUE RIDGE Information Systems Personnel Only)

28. BMC Remedy Action Request System Account created. YES ☐ NO ☐	29. Remedy Ticket #
30. Created By (Print and Sign)	31. Date (YYYY-MM-DD)
32. Verified By (Print and Sign)	33. Date (YYYY-MM-DD)

PART 5 (To be completed by Requestor)

34. Name (Last, First, Middle Initial)	35. DOD ID Number

36. **USER AGREEMENT -** STANDARD MANDATORY NOTICE AND CONSENT PROVISION:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any devise attached to this information system) that is provided for U.S. Government-authorized use only.
- You consent to the following conditions:
  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security, (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
    - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
    - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
    - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
    - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

37. Name (Last, First, Middle Initial)	38. DOD ID Number

(Block 36 Cont)

USER RESPONSIBILITIES:

I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN) required for logon authenticationat the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access bythe cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of a Navy informationsystem.
- Digitally sign and encrypt e-mail in accordance with current policies.
- Employ sound operations security measures in accordance with DOD, DON, service and command directives.

I further understand that, when using Navy IT resources, I shall not:

- Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., .com).
- Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, ProxyServers, Anti-Virus Programs).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
  Relocate or change equipment or the network connectivity of equipment without authorization from the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).
- Use personally owned hardware, software, shareware, or public domain software without written authorization fromthe Local IA Authority.
- Upload/download executable files (e.g., exe, .com, .vbs, or .bat) onto Navy IT resources without the written approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or Introduce malicious software, programs, or code.
- Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII, and other uses that are incompatible with public service.
- Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

39. Users Signature	40. Date (YYYY-MM-DD)

1. All personnel (military/civilian/contractor) working with USS BLUE RIDGE (BLR) domain IT systems will comply with the provisions listed herein. Non-compliance may result in the loss of Local Area Network (LAN) access; seizure of equipment and software; Personal Computer (PC) or both.

2. Your password is **FOR YOUR EYES ONLY** and will not be disclosed or used by anyone else regardless of the situation or circumstances. You will protect your password at the highest level of data it secures. You will NOT log on to a system and let another individual cleared or not use the system under you logon. Such disclosure to, or use by, another is considered a security violation and will result in your suspension from access to the system. Should you have reason to believe or are aware that your password has been compromised you must contact the Information System Security Manager (ISSM), regional Information System Security Officer (ISSO) or Network Administrators immediately. Passwords must be at least 15 characters long. Names and obvious words in your password: upper/lower case, numbers and special characters.

3. Users will **NOT** use software unless it has been tested and properly loaded onto the machine by BLR SCI ISSM personnel and is listed on the software inventory for that PC. The user will not violate any copyright or other license agreements and is responsible for reporting any known violation to the ISSM or ISSO. If privately owned or unauthorized software (i.e., games, screen savers etc.) are discovered on government owned PCs the software will be removed and a report submitted to the offender's chain of command by the ISSM or ISSO.

4. Government owned computers are not authorized for personal use. They are to be used for official business only.

5. **Physical access to the computer system at any given time is limited to those with a clearance and need-to-know for all information contained on that system.** Monitor screens, printers and other devices that produce human-readable output will be placed away from doors and windows. **Never leave a computer running unattended while it contains information that should not bee seen by anyone with physical access to it.**

6. **Printers should not be left unattended** while classified or sensitive by unclassified information is being printed unless the area in which it is located provides a level of physical security adequate to protect the printout from access by an unauthorized person. Any user who prints out classified or sensitive but unclassified information should remove the printout from the printer as soon as possible.

7. **Take caution with food and drink near computer systems.** Any spillage will seriously damage the system and/or magnetic media. Protect magnetic media from exposure to dust, magnetic fields, and liquid. Diskettes that get wet will generally warp or become otherwise deformed. If a diskette or volume of media does get wet, do not attempt to use it in the system or damage to the system will occur.

8. All removable media **(regardless of the source, content or application)** requires review and approval before being transferred to or from any BLR IT systems.

9. **Never alter the configuration files on any PC.**

10. Do Not shut down workstations unless directed by BLR IT personnel.

11. TOP SECRET (TS) or Special Compartmented Information (SCI) material is not authorized for generation or viewing from any GENSER LAN PC.

12. **DO NOT SEND PERSONAL GROUP EMAILS.** Only send group emails (e.g. All hands) is mission-related to all recipients.

13. **ALWAYS LOG OFF AT THE END OF THE DAY!**

14. In accordance with the Office of Director of National Intelligence (ODNI), all personnel must complete annual cyber awareness training in order to maintain access to Joint Worldwide Intelligence Communications System (JWICS). Users will complete either the Intelligence Systems Security Awareness (IC-ISSA) or DOD IC Cyber Awareness Challenge for the intelligence community in order to satisfy this FY requirement. Users accounts will be disabled when cyber awareness certificates are expired. User account will remain disabled until a valid cyber awareness certificate is provided to BLR IT Department. Authorized methods for training delivery are:

    (A) Navy Knowledge Online (NKO) portal,
    https://www.aas.prod.nel.training.navy.mil/ELIAASv2p/EV2NKOLoginListener
    (B) Total Workforce Management Service (TWMS),
    https://twms.navy.mil/selfservice/login.asp
    (C) DISA IA Training Portal,
    http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm

15. In accordance with CNSS 1253 Mar 2014 Appendix E, all user accounts which remain inactive for a period of 90 days will be disabled automatically. User accounts which remain inactive for a period 180 days will be deleted unless the user has given prior notification of extended inactivity due to deployment or TAD assignment.