SURFACE SHIP SUPPORT CENTER - SYSTEM AUTHORIZATION ACCESS REQUEST (SSSC - SAAR)

PRIVACY ACT STATEMENT

The information attached or contained within includes Personal Information under General Dynamics policy CP 07-105. This information can be accessed only by authorized personnel of General Dynamics and its approved service providers and may be used only as permitted by General Dynamics and its policies. Contractual restrictions apply to all third parties.

TYPE OF REQUEST	DATE (YYYYMMDD)
☐ Initial ☐ Modification ☐ Deactivate ☐ User ID _____	

SYSTEM NAME	LOCATION (Physical Location of System)
SSSC Website	**BIW Planning Yard, Brunswick, ME**

PART I (To be completed by Requester)

1. NAME (Last, First, Middle Initial)		2. SOCIAL SECURITY NUMBER (Last Four) **N/A**
3. ORGANIZATION	4. OFFICE SYMBOL / DEPARTMENT	5. PHONE (Include Country Code & Area Code)
6. OFFICIAL EMAIL ADDRESS		7. JOB TITLE AND GRADE / RANK
8. OFFICIAL MAILING ADDRESS		

9. ITAR ELIGIBILITY - Only U.S. Persons as defined in the International Traffic in Arms Regulations may have access to controlled technical data.
(a) I hereby certify that I am either a: (1)____Citizen of the United States of America, or a (2)____Lawful permanent resident ("Green Card" holder), employed by a company incorporated under the laws of the United States in accordance with the ITAR.
(b) Form of proof provided: Birth Certificate issued by/date/number_____,
US Passport/Passport Card #_____"Green Card" #_____Other-specify _____

10. USER SIGNATURE X	11. DATE (YYYYMMDD)

PART II ENDORSEMENT OF ACCESS BY USER SUPERVISOR, OR GOVERNMENT SPONSOR
(Contractors must provide a valid contract number and date of contract expiration in Block 12a & 12b)

12. JUSTIFICATION FOR ACCESS	12a. Contract Number
13. VERIFICATION OF NEED TO KNOW ☐ I hereby certify that this user has a valid requirement to access the SSSC Website.	12b. Contract Exp. (YYYYMMDD)

14. SUPERVISOR or SPONSOR NAME (Last, First, Middle Initial)	15. SUPERVISOR OR SPONSOR EMAIL ADDRESS	
16. ORGANIZATION	17. OFFICE SYMBOL / DEPARTMENT	18. PHONE (Include Country Code, Area Code)
19. SIGNATURE OF ENDORSEMENT (User supervisor, or government sponsor) X		20. DATE (YYYYMMDD)

21. NAME (Last, First, Middle Initial)	22. SOCIAL SECURITY NUMBER (Last Four) **N/A**

23. USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION

In order for Bath Iron Works (BIW) to pursue its business activities, BIW must protect its intellectual property and computer and network systems, including without limitation all hardware and software used in connection with such systems, all electronic information and files stored on, transmitted by or received by such systems, and all access information such as account names, access privileges and passwords (collectively, "BIW Information Assets").

In exchange for, and as a condition to, BIW granting me access to BIW Information Assets via the SSSC WEB SITE, I understand and agree to the following conditions of use:

- I will comply with all these BIW Information Security and Ethics Policies.
- I will not engage in, send, download, display, print, forward or otherwise disseminate or store material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, threatening or otherwise unlawful.
- I will not intentionally write, compile, copy, propagate, execute, or attempt to introduce any malicious computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system.
- I will not use personal devices to store or process business information.
- BIW has exclusive ownership of BIW Information Assets, and I have no ownership interest therein.
- I understand, Bath Iron Works Information Assets are provided for Bath Iron Works authorized personnel use only. Unauthorized access or use of Bath Iron Works Information Assets is forbidden, and may subject violators to criminal, civil, and/or administrative action.
- BIW Information Assets contain sensitive and proprietary business information and I will protect them in accordance with BIW and Government policies and procedures on information protection.
- I will not abuse or misuse my access privileges for any personal or private gain, nor will I compromise the BIW Information Assets to which I am granted access.
- I will not attempt to access areas other than those to which I have been specifically granted access.
- I will not divulge or share access information (such as account names, access privileges and passwords), unless authorized by BIW IT. I will maintain the secrecy and security of my access information, and will prevent others from using my access information without appropriate authorization.
- I will promptly report any/all problems or security violations regarding BIW Information Assets to the appropriate authorities (BIW/ CSCHelpdesk (207) 442-2400 and BIW Security (207)442-2280) immediately after becoming aware of such problems or violations.
- I will not install or otherwise use any software or hardware in connection with BIW Information Assets, except as provided by or expressly authorized by BIW.
- I will not disable or attempt to disable any security relevant system features without the authorization of the BIW Security organization.
- I will not send, store or process any Government classified information on any unclassified BIW Information Asset.
- I understand I have no expectation of privacy with the use of any BIW Information Assets. I further understand that my access and use of BIW Information Assets (including any online activities) may be monitored and audited by BIW at any time, and BIW may maintain records and logs of such access and uses.
- I understand, at any time, and without prior notice, BIW reserves the right to examine the contents of any Information Asset which includes but is not limited to e-mails, files, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through BIW Information Assets.
- Failure to agree to the conditions in this agreement will result in denial of access to BIW Information Assets.
- The restrictions in this Agreement regarding confidentiality and protection of BIW Information Assets shall continue to apply after the termination of my employment or business relationship with BIW, for any reason.

If, for any reason, I cannot comply with these requirements, I will immediately cease using or accessing BIW Information Assets until otherwise informed by BIW and will immediately inform the BIW Security (207)442-2280. I understand that if I violate the terms of this Agreement, or otherwise compromise BIW Information Assets, I may be subject to disciplinary action up to and including the User's termination of employment or loss of access to BIW Information Assets.

The restrictions in this Agreement regarding confidentiality and protection of BIW Information Assets shall continue to apply after the termination of my employment or business relationship with BIW, for any reason.

24. USER SIGNATURE X	25. DATE (YYYYMMDD)

26. NAME (Last, First, Middle Initial)	27. SOCIAL SECURITY NUMBER (Last Four) **N/A**

28. ITAR AGREEMENT

I understand and agree to comply with all U.S. Government regulations regarding the release of Technical Data.

In the event of any exchange with foreign nationals, I shall not disclose unauthorized technical data. I acknowledge and understand that any technical data or defense services related to defense articles on the U.S. Munitions List, to which I have access or that is disclosed to me in the course of my work with BIW is subject to export control under the International Traffic in Arms Regulations (ITAR) (title 22, code of Federal Regulations, Parts 120-130).

I hereby certify that such data or services will not be further disclosed, exported or transferred in any manner to any foreign national or any foreign country without prior written approval of the Office of Defense, Trade Controls, U.S. Department of State. Any disclosure or export shall be in accordance with an approved license from the U.S. Department of State and the U.S Customs Regulations.

28a. ITAR TRAINING REQUIREMENT

☐ I hereby certify that I have read and understood, my responsibility to protect ITAR controlled technical data as outlined in block 28 of this form.

29. USER SIGNATURE X	30. DATE (YYYYMMDD)

PART III REQUESTER'S SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

31. JOINT CERTIFICATION PROGRAM (JCP) CERTIFICATION NUMBER (Not required for government activities)	32. JCP EXPIRATION DATE (YYYYMMDD) (Not required for government activities)
33. TYPE OF BACKGROUND INVESTIGATION	34. INVESTIGATION DATE (YYYYMMDD)

35. CLEARANCE LEVEL	36. SECURITY MANAGER NAME (Last, First, Middle Initial)
37. SECURITY MANAGER TELEPHONE	38. SECURITY MANAGER EMAIL

39. SECURITY MANAGER SIGNATURE X	40. DATE (YYYYMMDD)

PART IV COMPLETION BY BIW AUTHORIZED STAFF

41. PLANNING YARD APPROVAL BY (PRINT NAME AND SIGN) X ☐ JCP CHECKED ☐ VISUAL COMPLIANCE	42. DATE (YYYYMMDD)
43. NAVY DATA OWNER APPROVAL (PRINT NAME AND SIGN) I hereby authorize access to the SSSC webpage. X	44. DATE (YYYYMMDD)
45. ACCOUNT PROCESSING COMPLETED BY (PRINT NAME AND SIGN) X	46. DATE (YYYYMMDD)

Mail, Email or fax completed SSSC-SAAR forms to: Attention: Data Manager

Mail:	Email:	Fax:
Bath Iron Works 700 Washington St. M/S 6520 Bath, ME 04530	**biwpydm@gdbiw.com**	**207-442-1912**

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.
(2) Social Security Number is not required you may leave this block empty.
(3) Organization. The user's current organization (i.e., USS xx, DoD, and government agency or commercial firm).
(4) Office Symbol/Department. The office symbol or department number within the current organization (i.e., D86).
(5) Telephone Number. The commercial phone number of the user including Country Code and Area Code.
(6) Official E-mail Address. The user's official e-mail address.
(7) Job Title/Grade/Rank. The civilian job title (i.e., Systems Analyst, YA-02, military rank (CAPT, United States Navy) or "CONT" if user is a contractor.
(8) Official Mailing Address. The user's official mailing address.
(9) ITAR Eligibility. Confirmation of the user's citizenship status. Only American citizens and Lawful permanent residents (Green Card Holders) are permitted access.
(10) User's Signature. User must sign the SSSC-SAAR with the understanding that they are responsible and accountable for their password and access to the system(s).
(11) Date. The date the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(12) Justification for Access. A brief statement is required to justify establishment of an initial USER ID.
(12a & 12b) Contract Number and Expiration Date is required for all contractors.
(13) Verification of Need to Know. To verify that the user requires access as requested.
(14) Supervisor or Sponsor Name (Print Name). The supervisor or government sponsor prints his/her name to indicate that the above information has been verified and that access is required.
(15) Supervisor or Sponsor E-mail Address. Official e-mail address of the user's supervisor or government sponsor.
(16) Organization. Supervisor or Sponsor's organization (i.e., USS xx, DoD, and government agency or commercial firm).
(17) Office Symbol/Department. The office symbol or department number within the supervisor or sponsor's current organization (i.e., D86).
(18) Phone Number. Supervisor or Sponsor's telephone number.
(19) Signature of Endorsement. Signature is required by either a government sponsor, or user's supervisor.
(20) Date. Date supervisor or sponsor signs the form.

C. COMPLIANCE AGREEMENTS: User must sign to indicate that he/she agrees to the terms and conditions of use.

(21) Name. The last name, first name, and middle initial of the user.
(22) Social Security Number is not required you may leave this block empty.
(23) User Agreement - Standard Mandatory Notice and Consent Provision. User must read and understand all information in this block.
(24) User Signature. User signature in this block denotes agreement with the terms and conditions listed in block 24.
(25) Date. The date the user signs the form.
(26) Name. The last name, first name, and middle initial of the user.
(27) Social Security Number is not required you may leave this block empty.
(28) ITAR Agreement. User must read and understand all information in this block.
(28a) ITAR Training Requirement. Confirmation of the user's training status. ITAR Training is required for all users.
(29) User Signature. User signature in this block denotes agreement with the terms and conditions listed in block 29.
(30) Date. The date the user signs the form.

D. PART III: Certification of Background Investigation or Clearance. This portion of the form should be completed by the user's local Security Management Office or equivalent organization. **Also required to validate ITAR Part I block 9**.

(31) Joint Certification Program (JCP) Certification Number. JCP Certification Number for the user's employer. Not required for government activities.
(32) JCP Expiration Date. Date of expiration for the JCP record of the user's employer. Not required for government activities.
(33) Type of Background Investigation. The user's last type of background investigation (i.e., NAC, NACI or SSBI).
(34) Investigation Date. Date of the user's last background investigation.
(35) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(36) Security Manager Name. Name of the Security Manager who has verified the user's information is correct.
(37) Security Manager Telephone Number. The telephone number of the Security Manager.
(38) Security Manager Email. The official email address of the Security Manager.
(39) Security Manager Signature. The Security Manager indicates that the above clearance and investigation information has been verified by signing block 40.
(40) Date. The date that the form was signed by the Security Manager.

E. PART IV: Completion by BIW Authorized Staff. No information should be entered into Part IV by the user, user's supervisor, government sponsor, or any other entity not specifically authorized to do so by BIW.

(41) Planning Yard Approval. Signature in this block denotes Planning Yard staff review of the application. By placing checks in the "JCP Checked" and "Visual Compliance" Planning Yard staff confirms that JCP and Visual Compliance have been verified for user application.
(42) Date. The date that the form was signed by Planning Yard Approval Staff.
(43) Navy Data Owner Approval. Signature in this block denotes Navy Data Owner approval for the user application.
(44) Date. The date that the form was signed by the Navy Data Owner.
(45) Account Processing Completed. Signature in this block denotes that final Account Processing has been complete. No further action is required for this application.
(46) Date. The date that the form was signed by the Account Processing Staff.