U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave, SE
Stop: 7501
Washington, DC 20593-7501
Staff Symbol: (BSX-1)
Phone: (202) 372-1261
Fax: (202) 372-1920
Email: CGAUX@uscg.mil

16790 / AUX-PL-020(A)
BSX Policy Letter 22-10
12 May 2022

MEMORANDUM

From: /T. P. Glendye, CAPT/
Chief, Office of Auxiliary and Boating Safety

Reply to Attn of: CG-BSX-11
LT Christopher Booth
(202) 372-1056

To: Distribution

Subj: AUXILIARY DATABASE (AUXDATA II) INFORMATION SYSTEM ACCESS

Ref: (a) Auxiliary Manual, COMDTINST M16790.1 (series)
(b) BSX Policy Letter 19-4, Auxiliary Database (AUXDATA) Information System Access, of 12 Jul 19

1. PURPOSE. This policy letter defines criteria, requirements, and procedures for managing system access and account permissions in the Auxiliary Database (AUXDATA II) information system in accordance with reference (a). Its provisions shall also be applicable to any successor to AUXDATA II upon system activation.

2. ACTION. All Coast Guard Auxiliarists, District Director of Auxiliary (DIRAUX) offices, and other Coast Guard units and offices managing Auxiliary activities with AUXDATA II shall comply with the provisions in this Policy Letter as defined in Enclosure (1).

3. DIRECTIVES AFFECTED. This Policy Letter supersedes reference (b).

4. BACKGROUND. AUXDATA II replaced the legacy AUXDATA and Auxiliary Order Management (AOM) systems in April 2020 and became the Coast Guard's information system of record for its Auxiliary program. It is the repository for data of both a personal and activity-based nature for active and retired members of the Auxiliary. Additionally, it is the patrol order and facility management system for the Auxiliary.

5. DISCLAIMER. This Policy Letter is not a substitute for applicable legal requirements, nor is it a rule. It is intended to define Auxiliary database access and data management requirements for Coast Guard and Coast Guard Auxiliary personnel and is not intended to, nor does it impose legally-binding requirements on any party outside the Coast Guard.

6. MAJOR CHANGES. Major changes revolve around dissemination of licenses and permission sets that were not applicable to the previous system.

7. DISTRIBUTION. No paper distribution will be made of this Policy Letter. An electronic version will be posted on the Chief Director of Auxiliary (CHDIRAUX) and Coast Guard Auxiliary web sites: http://agroup-bx.wow.uscgaux.info/content.php?unit=BX-GROUP and http://www.cgaux.org/, respectively. All web sites in this Policy Letter are the most current available. If the cited web link does not work, then access should be attempted by copying and pasting or typing the web site address into the user's internet browser.

8. QUESTIONS. Questions about this Policy Letter should be submitted in writing to the cognizant Auxiliary chain of leadership and management.

9. REQUESTS FOR CHANGES. Requests for changes to this Policy Letter should be submitted in writing via the cognizant Auxiliary chain of leadership and management. Relevant portions of this Policy Letter will be incorporated in the next change to reference (a).

#

Dist: CG-761, CG-681, C5ISC, DIRAUX (dpa), NEXCOM, ANACO-IT

Encl: (1) AUXDATA II Information System Access Guidelines

AUXDATA II Information System Access Guidelines

Table of Contents

1. Overview of Database Environments, Account Types, and Licenses.

   a. There are four AUXDATA II database environments:

      (1) The Development (Dev) environment facilitates research and development of data creation, storage, retrieval, and update capabilities.

      (2) The Quality Assurance (QA) environment facilitates development of test plans and expected results of potential changes to AUXDATA II before final testing.

      (3) The User Acceptance Testing (UAT) environment facilitates testing of user stories to ensure accurate functionality and capability before being finalized in AUXDATA II.

      (4) The Production (Prod) environment is the primary database for all users. Once ready for full implementation, changes are institutionalized in the production database.

   b. Due to the presence of Personally Identifiable Information (PII) in AUXDATA II, login to the Prod environment requires Two-Factor Authentication (2FA). The UAT environment is periodically updated to match the production database.

   c. There are two types of AUXDATA II accounts:

      (1) Licensed Accounts. Licensed account holders have the ability to create, read, update, retrieve, and delete all data and data elements, as well as create, update and delete data elements and user permissions. The Chief Director of Auxiliary (CHDIRAUX), through their Auxiliary Division designees (CG-BSX-1), is responsible for creating and managing licensed accounts. This responsibility may not be delegated.

      (2) Community User Accounts. Community user account holders have the ability to create, read, update and retrieve selected data based on the permissions granted for their accounts. Coast Guard Finance Center staff who require access to AUXDATA II may be provided read-only community user accounts.

   d. AUXDATA II user licenses are intended and assigned for individual use. Group or shared accounts are not used within AUXDATA II. Since there are no group or shared accounts, there are no requirements to terminate account credentials for accounts that do not exist (i.e., if a group member were to leave a group). Once a user's account is created, they will be notified via email to log into the system. Any actions a user takes inside the system will be tracked via an audit log. Users will also be notified via email of modifications made to their account.

   e. AUXDATA II user accounts and permissions shall be reviewed annually by the

AUXDATA II Configuration Advisory Board (CAB) and approved by CG-BSX-1. Permissions shall only be added or removed to ensure the user has just the necessary access to perform required tasks.

f. AUXDATA II user accounts that have not been used in over 90 days will be deactivated. Requests to reactivate inactive accounts shall be forwarded to the cognizant DIRAUX per District policies for DIRAUX communications.

.

g. Login instructions for users are as follows:

(1) Access the AUXDATA II login page.

(2) Input user name and password.

(3) Read and select "Acknowledge" on the DoD banner.

(4) Select multi-factor authentication method (one-time password or Salesforce Authenticator Application).

(5) Enter the one-time password to access the system.

2. Account Management.

a. Licensed Account Holders.

(1) CG-BSX-1, Executive Assistants (EA) to the CHDIRAUX for AUXDATA II management (AUXDATA II EA), and selected DIRAUX staff are granted licensed accounts with full data management privileges and permissions. They are also delegated the authority to create and manage Community User Accounts for Auxiliarists, DIRAUX staff including Operations Training Officers (OTOs), Order Issuing Authorities (OIAs), and any other potential AUXDATA II user in need of direct access to information residing in AUXDATA II.

(2) This designated authority may not be re-delegated except as defined in this Policy Letter. Questions that may arise from these provisions, or determinations that need to be made about them, shall be resolved by CG-BSX-1.

b. Community User Account Holders.

(1) DIRAUX are authorized to create Community User Accounts in the production database for all Auxiliarists in their respective regions, as well as create such accounts for Coast Guard offices and units requiring AUXDATA II access. Accounts shall remain active until the account holder no longer requires the account (e.g., due to an Auxiliarist's retirement or disenrollment; due to a Coast Guard office's completion of a project that required AUXDATA II access, completion of a transfer or retirement, etc.) or if the account is suspended pursuant

to other DIRAUX action.

(2) All Auxiliarists shall have a Community User Account with limited ability to manage data. The cognizant DIRAUX shall create accounts for all Auxiliarists upon their enrollment.

(3) Community User Account holders serving in specific organizational roles may be granted enhanced privileges and permissions to manage data and information within their area of responsibility (e.g., the District Staff Officer for Aviation (DSO-AV) who reviews and endorses aircraft facility offers for use). Should Coast Guard personnel or Auxiliarists require such enhanced privileges and permissions in order to complete specific tasking, then a request for such must be submitted via the DIRAUX to CG-BSX-1 (Tier 1 service request preferred; email acceptable). Should the request be approved, the permission will be documented in AUXDATA II through the service request process.

c. Account Management in Database Environments.

(1) Dev Environment. Access to the Dev environment shall be managed by CG-BSX-1 and shall normally be limited to no more than two licensed account holders.

(2) QA Environment. Access to the QA environment shall be limited to CG-BSX-1, AUXDATA II EAs, and members of the AUXDATA II Configuration Advisory Board.

(3) UAT environment. Community User Account holders in the Prod environment who have been identified by CG-BSX-1 and the Assistant National Commodore for Information Technology (ANACO-IT) as User Acceptance Testers may have either a Community User Account or an enhanced account in UAT similar to that of a Licensed Account. On a case-by-case basis as determined by CG-BSX-1, accounts may be granted in UAT to facilitate training. Requests for UAT access outside of national staff and CG-BSX-1 shall be submitted as a Tier 1 service request.

(a) Access to UAT for training purposes shall be limited to CG-BSX-1, AUXDATA II EAs, and AUX-10 C-school instructors. Accounts may also be granted to facilitate training of Information Services (IS) staff officers. Such access shall only be granted to facilitate AUX-10 C-School training of IS staff officers required for the activity approval permission. The Auxiliary national Division Chief for IS Officer Support (DVC-UI) is authorized to manage IS staff officer training accounts in UAT.

(b) Access to UAT shall only be granted to C-school students for a period no more than 60 days prior to a class and not to exceed 60 days after class completion. Instructors for the Information Systems (AUXDATA II) C-school (AUX-10) shall have continual access for as long as they are AUX-10

instructors unless suspended or terminated as determined by CG-BSX-1.

(c) On a case-by-case basis as determined by CG-BSX-1, access to UAT may also be granted to facilitate training of coxswains and coxswain trainees. Such access shall only be granted to facilitate training in the patrol order and patrol activity processes. The Auxiliary national Division Chief for AUXDATA II Support (DVC-UD) is authorized to manage coxswain/coxswain trainee training accounts in UAT. Access shall only be granted for a period no more than 90 days.

(4) Prod Environment. Access to the Prod environment shall be primarily managed by DIRAUX. CG-BSX-1 and AUXDATA II EAs are also authorized to manage such access.

d. Atypical account usage. The majority of users of AUXDATA II are Auxiliary members who do not have a consistent or defined schedule of use for the system. Due to AUXDATA II's user base, atypical usage is difficult to define. The following definition applies to AUXDATA II atypical account usage: Multiple login attempts by the same user. If such occurrence is identified as atypical usage and not user error, it must be reported to the ISSO immediately.

3. Account Suspensions and Revocations.

a. Any user account shall be immediately suspended by CG-BSX-1, AUXDATA II EAs, or DIRAUX (or OTO in the absence of the DIRAUX) in any of the following circumstances:

(1) The account holder demonstrates behavior observed first-hand or as reported by a third party (telephonic or email acceptable) that compromises or may compromise the integrity of AUXDATA II, may be detrimental to the good order and proficient operation of AUXDATA II in any way, or gives rise to the request and justification by any higher authority of the account holder in question (telephonic or email acceptable); or,

(2) The account holder demonstrates behavior observed first-hand or as reported by a third party (telephonic or email acceptable) that may be inconsistent with the high levels of trust and integrity expected of an AUXDATA II user, or gives rise to the request and justification by any higher authority of the account holder in question (telephonic or email acceptable); or,

(3) Suspension action is otherwise directed by a Coast Guard authority (e.g., suspension directed by the District Commander or CG Cyber Command).

b. Any user account shall be immediately revoked via a Tier 1 service request in AUXDATA II by CG-BSX-1, AUXDATA II EAs, or DIRAUX (or OTO in the absence of the DIRAUX) in any of the following circumstances:

(1) The account user requests their account to be revoked; or,

(2) The account user no longer serves in a role that requires the account, for any reason (e.g., non-reappointment, removal, resignation); or,

(3) The account holder demonstrates behavior observed first-hand or as reported by a third party (telephonic or email acceptable) that compromises or may compromise the integrity of AUXDATA II, is detrimental to the good order and proficient operation of AUXDATA II in any way, or gives rise to the request and justification by any higher authority of the account holder in question (telephonic or email acceptable); or,

(4) The account holder demonstrates behavior observed first-hand or as reported by a third party (telephonic or email acceptable) that is inconsistent with the high levels of trust and integrity expected of an AUXDATA II user, or gives rise to the request and justification by any higher authority of the account holder in question (telephonic or email acceptable); or,

(5) Revocation action is otherwise directed by a Coast Guard authority (e.g., directed by the District Commander or CG Cyber Command).

c. For the above purposes, higher authority is defined as follows:

(1) The elected leader at a staff officer's organizational level (e.g., for a flotilla member it would be the Flotilla Commander (FC); for a District Commodore (DCO) it would be the appropriate Deputy National Commodore (DNACO); for a DNACO, it would be the Vice National Commodore (VNACO)); or,

(2) The appointed officer at a staff officer's next highest organizational level (e.g., for a Division IS Officer (SO-IS) it would be the District IS Officer (DSO-IS); for the Division Chief for IS Officer Support (DVC-UI) it would be the Director, IT User Support and Services (DIR-U)); or,

(3) The DIRAUX, DCO, or DSO-IS for any Auxiliarist within their Auxiliary region; or,

(4) The CHDIRAUX, CG-BSX-1, National Commodore (NACO), DNACO for Information Technology and Planning (DNACO-ITP), ANACO-IT, Director of Information Technology User Support and Services (DIR-U), or DVC-UI for any individual at national staff level, or at regional level only after advising the cognizant DIRAUX and DCO (email acceptable);

(5) The cognizant instructor of the individual who has been granted access.

(6) Any Coast Guard Commissioned Officer, Warrant Officer, or Officer-in-Charge.

d. Upon suspension of any user account, the entity taking the suspension action shall immediately notify the user of such action in writing (email acceptable), copy as appropriate to the user's DIRAUX, DSO-IS, and at least one AUXDATA II EA. If the user is a national staff member, then notification shall also be made to the DVC-UI and the appropriate Directorate Chief (DIR).

4. General Guidelines for Enhanced Account Permissions in Production.

a. In determining whether or not a community user requires additional permissions in the Prod environment beyond what is provisioned in their account, the primary consideration is the individual's organizational position.

(1) Justification for enhanced data management permissions is strongest for DIRAUX Administrative Assistants (D-AA).

(2) Justification for selected enhanced data management permissions is strongest for OIAs and IS officers because of the specific nature of their activity approval functions.

(3) Justification for specific role-based permissions is limited to users with a need to manage a specific program area or perform a step in an AUXDATA II workflow process (e.g., assignment of an HF radio facility call sign by the Branch Chief for Integration in the Response Directorate (BC-RTI)).

b. The scope of AUXDATA II permissions that may be granted shall be limited to no higher and no broader than the organizational level and data management responsibilities of the user to whom it is being granted.

c. Requests for additional permissions or permission changes shall be processed through a DSO-IS, an AUXDATA II EA, or CG-BSX-1 as follows;

(1) If the changes are requested through a DSO-IS then the DSO-IS shall do so via a Tier 1 AUXDATA II Service Request. The request shall be assigned to an AUXDATA II EA for review and approval. If the AUXDATA II EA has any question or concern about granting additional permissions to any individual, they shall first consult with the individual's cognizant DIRAUX, District Chief of Staff (DCOS), or ANACO if a member of national staff, as appropriate to resolve the concern. The basis of their approval or denial of the request shall include consideration of their assessment of the consultation.

(2) If the changes are requested through an AUXDATA II EA then the AUXDATA II EA shall do so via direct request to CG-BSX-1 (email acceptable). If CG-BSX-1 has any question or concern about granting additional permissions to any individual, they shall first consult with the individual's cognizant DIRAUX, DCOS, or ANACO if a member of national staff, as appropriate to resolve the concern. The basis of their approval or denial of the request shall include consideration of their

assessment of the consultation.

(3) CG-BSX-1 may authorize additional permissions or permission changes. If CG-BSX-1 has any question or concern about authorizing additional permissions to any individual, they shall first consult with the individual's cognizant DIRAUX, DCOS, or ANACO if a member of national staff, as appropriate to resolve the concern. The basis of their approval or denial of the request shall include consideration of their assessment of the consultation.

(4) Upon granting of additional or changed permissions to an individual, the requestor shall notify the individual of such action in writing (email acceptable) and copy the cognizant DSO-IS and DIRAUX, DVC-UI, appropriate DIR if for a member of national staff, and CG-BSX-1 if appropriate (e.g., if an AUXDATA II EA was the requestor).

(5) AUXDATA II EAs shall immediately revoke AUXDATA II permissions from anyone in the same manner as user account revocations defined in paragraph 3.b.

(6) Upon removing AUXDATA II permissions, the AUXDATA II EAs shall notify the individual of such action in writing (email acceptable) and copy the cognizant DSO-IS and DIRAUX, DVC-UI, appropriate Directorate Chief if for a national staff member, and CG-BSX-1 if appropriate.

5. Granting, Maintaining, and Removing Activity Approval Permissions in Production.

a. Activity approval permission or permission changes shall be requested via a Tier 1 AUXDATA II Service Request by a DSO-IS.

(1) AUXDATA II EAs shall be designated members of the Tier 1 Service Request Team in order to use the AUXDATA II Permissions category to process such requests.

(2) AUXDATA II EAs shall review requests in new, in-process, hold, or closed status and appropriately self-assign them or assign them to another EA if necessary.

(3) Once so assigned, an AUXDATA II EA shall process each request for review and approval, and in the process create a permanent processing history by documenting all actions taken in the service request. An Access Permissions Memo will be issued by CHDIRAUX to the Auxiliarist receiving the activity log approval permissions (Appendix B).

b. Activity approval permissions shall only be granted to Auxiliarists who meet the following requirements and who require such access for their performance of duty as appointed IS officers at any organizational level:

(1) Successful completion and currency in all Auxiliary Core Training (AUXCT)

requirements; and,

(2) Current favorable Operational Support (OS) background check; and,

(3) Successful completion of one of the following four training options (successful completion is defined as achieving a score of at least 90 percent on an end-of-instruction exam which has been approved by the DVC-UI):

(a) The in-residence Auxiliary Information Systems Training (AUX-10) C-school as reflected by AUXDATA II entry; or,

(b) An in-residence AUX-10 Auxiliary region-level course as reflected by AUXDATA II entry. Such course must be taught by at least one national AUX-10 instructor and at least one of a cadre of knowledgeable and experienced members who have been selected by the DSO-IS and approved by the DCO. The course must also be approved by the DVC-UI; or,

(c) An AUX-10-based virtual AUXDATA II IS course taught by at least one National AUX-10 instructor and reflected by AUXDATA II entry. Such course must be approved by the DVC-UI; or,

(d) An interim AUX-10-based Auxiliary region-level workshop taught by at least one of a cadre of knowledgeable and experienced members who have been selected by the DSO-IS and approved by the DCO. Such workshops must be approved by the DVC-UI, and its successful completion must be confirmed by the DSO-IS. This training option shall only be acceptable when an urgent need for AUXDATA II activity approval exists as determined by the DSO-IS and with the concurrence of the DIRAUX. The workshop's instruction material must be obtained from the DVC-UI. Resultant access shall only be granted for a period not to exceed one year during which the Auxiliarist must complete either 5.b.(3) (a), 5.b.(3) (b), or 5.b.(3) (c) above in order to retain access. Their activity approval permission shall be immediately removed if not successfully completed within that time period.

c. AUXDATA II EAs are not authorized to grant activity approval permission to individuals who are not serving as IS officers unless specifically directed by the cognizant DIRAUX or CG-BSX-1. Requests for non-IS officers to have activity approval permission must be submitted with justification by the requestor in writing to the cognizant DIRAUX or CG-BSX-1 (email acceptable).

6. Guidelines for Granting Activity Approval Permissions at Organizational Levels.

a. Flotilla level.

(1) AUXDATA II EAs are authorized to grant activity approval permission to the Flotilla Staff Officer for IS (FSO-IS) as requested and justified by the DSO-IS.

Requests should be made via a Tier 1 Service Request in AUXDATA II. Activity approval and management of member and unit information by the FSO-IS shall be limited in scope to the flotilla to which the FSO-IS is assigned. No other flotilla elected or appointed officer or other member may be authorized such permission. Visibility of user security information is not authorized. The DSO-IS shall maintain a report in AUXDATA II of all district FSO-IS who have activity approval permission. This responsibility may be delegated to an ADSO-IS.

(2) Flotilla IS officers shall not approve activity or manage other Auxiliary member or unit information. The only exceptions shall occur when an FSO-IS, as identified by their SO-IS, assists with division-wide data input and activity approval.

(3) The DSO-IS shall advise the individual to whom permission is granted that they must notify the DSO-IS when their permission is no longer needed, including when their office appointment ends. Whenever otherwise determined that the individual is no longer serving as the FSO-IS, their permission shall be removed immediately via a Tier 1 Service Request in AUXDATA II.

(4) In the event of a temporary FSO-IS vacancy (e.g., due to severe injury/illness or death), FSO-IS functions shall be assumed by the respective SO-IS until the FSO-IS is able to resume their functions or a new FSO-IS is trained and appointed. The SO-IS shall notify the DSO-IS whenever such vacancy occurs and when it is resolved (email acceptable).

b. Division level.

(1) As needed, AUXDATA II EAs are authorized to grant activity approval permission to the SO-IS as requested and justified by the DSO-IS. Requests should be made via a Tier 1 Service Request in AUXDATA II. Activity approval and management of member and unit information by the SO-IS shall be limited in scope to the division and its flotillas to which the SO-IS is assigned. No other division elected or appointed officer or other member may be authorized such permission except for prospective SO-IS replacements when necessary to prepare them for SO-IS functions. Visibility of user security information is not authorized. The DSO-IS shall maintain a report in AUXDATA II of all district SO-IS who have activity approval permission. This responsibility may be delegated to an ADSO-IS.

(2) Division IS officers shall not approve activity or manage other Auxiliary member or unit information. The only exceptions shall occur when an SO-IS, as identified by their DSO-IS, assists with district-wide data input and activity approval and no other Assistant DSO-IS (ADSO-IS) is available.

(3) The DSO-IS shall advise the individual to whom permission is granted that they must notify the DSO-IS when their permission is no longer needed, including when their office appointment ends. Whenever otherwise determined that the

individual is no longer serving as the SO-IS, their permission shall be removed immediately via a Tier 1 Service Request in AUXDATA II.

(4) In the event of a temporary SO-IS vacancy (e.g., due to severe injury/illness or death), the DSO-IS shall identify another qualified IS officer to assume the SO-IS functions until the SO-IS is able to resume their functions or a new SO-IS is trained and appointed. The DSO-IS shall coordinate with the unit leader regarding notification to DIRAUX when a vacancy occurs and when it is resolved (email acceptable).

c. District level.

(1) As needed, AUXDATA II EAs are authorized to grant activity approval permission to the DSO-IS as requested and justified by the DCO with concurrence of the DIRAUX. Activity approval and management of member and unit information shall be limited in scope to the district and its divisions and flotillas to which the DSO-IS is assigned. No other district elected or appointed officer or other member may be authorized such permission except for an ADSO-IS who is identified as the primary DSO-IS replacement described in paragraph 6.c.(3) below. If visibility of user security information is requested, that authorization must first be specifically approved by CG-BSX-1. CG-BSX-1 shall maintain a report in AUXDATA II of all DSO-IS and any other members who have activity approval permission.

(2) District IS officers shall not approve activity or manage other Auxiliary member or unit information outside their district.

(3) All DSO-IS shall identify an ADSO-IS to be ready as their primary replacement in the event of their temporary vacancy (e.g., due to severe injury/illness or death) and notify the DCO and DIRAUX in the event of a temporary vacancy. If an ADSO-IS has not been so identified when a vacancy arises, then the DCO shall identify another qualified IS officer to assume the DSO-IS functions until the DSO-IS is able to resume their functions or a new DSO-IS is trained and appointed.

(4) AUXDATA II EAs are authorized to grant additional district-level permissions to the DIRAUX and their designated staff, as requested and justified by the DIRAUX. Such permissions shall be limited in scope to the district and its divisions and flotillas to which the staff are assigned. Visibility of user security information is authorized. DIRAUX offices may activate the DIRAUX Administrative Assistant (D-AA) permission set for Auxiliarists who augment the DIRAUX office as Administrative Assistants. The permission set itself is managed by CG-BSX-1. Requests for additional permissions for D-AAs should be made to CG-BSX-1. Whenever an Auxiliarist is no longer serving as a D-AA, the permission set should be deactivated for that member.

(5) AUXDATA II EAs shall advise the individual to whom access is granted that they

must notify the AUXDATA II EAs when their access is no longer needed, including when their office appointment or assignment to the DIRAUX office ends. Whenever otherwise determined that an individual is no longer serving as the DSO-IS or assigned to the DIRAUX office, their access shall be immediately terminated. Termination requests should be made via a Tier 1 Service Request in AUXDATA II.

d. National level.

(1) AUXDATA II EAs are authorized to grant national level data management and activity approval permissions to Auxiliarists who augment the CHDIRAUX staff, as requested and justified by CG-BSX-1. If visibility of user security information is requested for anyone, authorization must first be specifically granted by CG-BSX-1.

(2) AUXDATA II EAs are authorized to grant limited role-based permissions to selected national staff officers who hold specific positions having a program management role, as requested and justified by the respective national staff officer through their DNACO. An example is management of Interpreter Corps language skills by the Director and Deputy Director for International Affairs. If visibility of user security information is requested for anyone, that authorization must first be specifically approved by CG-BSX-1

(3) AUXDATA II EAs shall advise the individual to whom permissions are granted that they must notify the AUXDATA II EAs when their permissions are no longer needed, including when their augmentation of the CG-BSX-1 staff ends. Whenever it is determined that the individual is no longer so assigned, their permissions shall be immediately deactivated. Termination requests shall be made via a Tier 1 Service Request in AUXDATA II.

(4) AUXDATA EAs shall notify CG-BSX-1 whenever they expect to be absent from their ability to perform their duties for a prolonged period of time.

e. Revocations shall be made in accordance with guidance in paragraph 3.b.

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave, S.E.,STOP 7501
Washington, DC 20593-7501
Staff Symbol: CG-BSX
Phone: (202) 372-1260

16970
XX YYY 20ZZ

Appendix A

MEMORANDUM

From: T. P. Glendye, CAPT
Chief, Office of Auxiliary and Boating Safety

Reply to Attn of: CG-BSX-11
LT C. Booth
(202) 372-1056

To: XXXXXXXXX

Subj: AUXDATA II ACCESS PERMISSIONS

Ref: (a) Auxiliary Manual, COMDTINST M16790.1 (series)
(b) CHDIRAUX Policy Letter 22-10 of 12 May 2022

1. In accordance with references (a) and (b), you are hereby granted additional access permissions in the Auxiliary Database (AUXDATA II).

2. You have been granted this additional permission(s) based on a stated need (INSERT DESIRED NEED FOR AUXDATA II PERMISSION(S)). You are to only use the granted permissions for your stated need, and any other actions within the AUXDATA II system must be granted in writing before such actions are taken. You are hereby granted permissions in AUXDATA II for the following:

a. INSERT SPECIFIC PERMISSIONS

b. INSERT SPECIFIC PERMISSIONS

3. This grant remains in effect until revoked or upon your request.

4. LT Chris Booth (Assistant Chief, Administration Branch / CG-BSX-11 / Christopher.w.booth@uscg.mil / 202-372-1056), or his successor, is your primary point-of-contact in the conduct of the aforementioned provisions.

#

Copy: Applicable Program Office

Appendix B

Acronyms

ADSO	Assistant District Staff Officer
ANACO	Assistant National Commodore
AUXCT	Auxiliary Core Training
AUXDATA	Auxiliary Database
BC-RTI	Branch Chief for Integration in the Response Directorate
CAB	Configuration Advisory Board
CG-BSX	Office of Auxiliary and Boating Safety
CG-BSX-1	Auxiliary Division
CHDIRAUX	Chief Director of Auxiliary (CG-BSX)
D-AA	District Director of Auxiliary Administrative Assistants
DCO	District Commodore
DIR	Directorate Chief
DIRAUX	Director of Auxiliary
DNACO	Deputy National Commodore
DSO	District Staff Officer
DVC	Division Chief
EA	Executive Assistant
FSO	Flotilla Staff Officer
IS	Information Services
ISSO	Information System Security Officer
IT	Information Technology
ITP	Information Technology and Planning
NACO	National Commodore
OIA	Order Issuing Authority
OS	Operational Support (background check)
OTO	Operations Training Officer
PII	Personally Identifiable Information
SO	Division Staff Officer
SPII	Sensitive Personally Identifiable Information
2FA	Two-Factor Authentication
UAT	User Acceptance Testing
UD	AUXDATA II Support
UI	IS Officer Support Division
VNACO	Vice National Commodore