DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5230.4B
N6
9 Aug 17

CNATRA INSTRUCTION 5230.4B

Subj: CHIEF OF NAVAL AIR TRAINING POLICIES AND GUIDELINES FOR INTERNATIONAL MILITARY PERSONNEL ACCESSING DEPARTMENT OF THE NAVY INFORMATION SYSTEMS RESOURCES

Ref: (a) CNATRAINST 5200.9A
(b) CNATRAINST 5239.3A
(c) CJCSM 6510.01B
(d) DOD 5220.22-M
(e) DODD 3020.40
(f) DODD 5230.20
(g) DODD 8500.01
(h) DODI 5200.02
(i) DODI 8510.01
(j) DODM 5200.1, V3
(k) OPNAVINST 5239.1C
(l) SECNAVINST 4950.4B
(m) SECNAVINST 5239.3B
(n) SECNAVINST 5510.30B
(o) SECNAVINST 5510.
(p) SECNAVINST 5510.34A

Encl: (1) List of Web Links to References
(2) OPNAV-5239-14-SAAR-N

1. Purpose. To provide Command policies and guidelines for International Military personnel access requirements and allowances to the unclassified Chief of Naval Air Training (CNATRA), Navy Flight Demonstration Squadron (NFDS)/Blue Angels and Naval Air Training Command (NATRACOM) Information Systems (IS) and networks to meet the requirements of references (a) through (p). Refer to Enclosure (1) for links to specific references. To issue policies and guidelines necessary for CNATRA to be consistent and effective in the implementation of these access requirements and allowances throughout CNATRA and NATRACOM. To apply basic policies and principles of administrative guidelines as they relate to Information Management and Information Technology (IMIT) and IS associated with and connected to the CNATRA, NFDS/Blue Angels and NATRACOM networks.

2. Cancellation. CNATRAINST 5230.4A

3. Objectives

a. Define International Military personnel as they are assigned to CNATRA, NFDS/Blue Angels or NATRACOM units and the IS access privileges they are allowed.

b. Describe the government requirements for requesting access and protecting data.

c. Provide guidance on the monitoring of International Military personnel and their IS access behaviors.

4. Authority. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with Department of Defense (DOD) and Department of Navy (DON) Cybersecurity policy and guidance for IS, reference (a) identifies this authority. Reference (b) identifies CNATRA's Cybersecurity Policy and Guidelines. Reference (g) provides specific guidelines for Cybersecurity policies. Reference (c) provides additional interactive understanding between directives, instructions and guidelines. The policies, procedures and principles presented in references (a) through (p) apply to all personnel assigned to CNATRA, NFDS/Blue Angels or NATRACOM units and all military, Government Civilians, (including Government Contractors and International Military personnel) who use IS resources within CNATRA, NFDS/Blue Angels or NATRACOM units. Reference (p) is Navy's policy on disclosures of Classified Military Information (CMI) and Controlled Unclassified Information (CUI) to Foreign Governments, International Organizations and Foreign Representatives.

5. Policy

a. International Military Personnel (IMP). The term International Military personnel will refer to all individuals who are non-United States (U.S.) Citizens. This is broken down into several groups:

(1) International Military Student (IMS) personnel are periodically assigned to NATRACOM units. IMS Aviation Pilots, Naval Flight Officers and Flight Surgeons training flight students and Instructors under Foreign Military Sales (FMS),

Professional Military Education (PME) and or other DOD International Military Education and Training (IMET) funded programs that are sponsored by the U.S. Government, DOD, Navy International Program Office (Navy IPO), Naval Education and Training Security Assistance Field Activity (NETSAFA) and are guided under reference (l), Joint Security Cooperation Education and Training (JSCET).

(2) North Atlantic Treaty Organization (NATO) or Foreign Exchange Officers are international military personnel who are occasionally assigned to NATRACOM units for a 12 to 36 month tour as an Instructor in an authorized billet under the Personnel Exchange Program (PEP), PME program and also assigned as the Country Liaison Officer. These Foreign Exchange Officers will be issued Invitational Travel Orders (ITO's) documenting the length of their stay and their appropriate security clearances. The decision to authorize these personnel a user account with access to the unclassified Next Generation Enterprise Network (NGEN), the TRANET-U networks and Training Integrated Management System (TIMS) rests with the Command granting access and should be based on the international military personnel's duties, need for access, meeting DON Personnel Security Program requirements and DON IA and Security Program regulations. A Common Access Card (CAC) will be provided to these personnel with a Foreign Identification Number (FIN) to allow for complete Cryptographic Log On (CLO) enforcement.

b. Government Requirements for Information System Access

(1) ITO'S are prepared and issued by the U.S. Government, specifically the Security Cooperation Office (SCO) for each foreign country. The ITO authorizes eligibility and access to unclassified DOD and DON IS for DOD and DON training courses listed and authorized in the ITO. This information is used to determine the appropriate IT position category. In-country U.S. officials will perform a security screening of each student prior to issuance of the ITO regardless of the level of classification of the training. The level of security clearance will be shown in item 11 of the ITO by selecting both statements (a) and (b) as shown below:

(a) "U.S. security screening has been accomplished. All training will be conducted on an unclassified basis."

(b) "U.S. security requirements have been complied with. The home government has granted the IMS a security clearance. This in and of itself does not permit the disclosure of classified U.S. information. Such disclosure must be specifically authorized by an official delegated authority and U.S. foreign disclosure regulations or directives." The level of the security classification granted by the home government will be indicated in block 11 (1) of the ITO and the U.S. equivalent classification level will be shown in block 11 (2) of the ITO.

(2) A completed SAAR-N, enclosure (2), must be signed by the IMP and routed through the Training Air Wing (TRAWING) IMSO and local site Security Manager, prior to account creation. The TRAWING IMSO will assist with completing the SAAR-N form and make the following statement on the Block 11, Justification for Access: "IMS is eligible and authorized to access Unclassified DON Level II IT systems and designation while enrolled and attending naval training and courses listed and authorized by his/her ITO". These forms are maintained on site with the Information Systems Security Officer (ISSM) until the IMP departs. Forms are then stored at CNATRA Headquarters (HQ) for six years and then destroyed appropriately.

(3) A current Cybersecurity Awareness and Personally Identifiable Information (PII) Training certificate is required prior to account creation.

(4) Accounts for IMP need to be identified by adding their country code to their email address and username on NGEN and in the DESCRIPTION field of the TRANET-U Active Directory (AD) accounts.

(5) The account is created after all requirements have been met, using the FIN as the CLO enforcement and expiration date of time frame of the tour of duty.

(6) After the student departs, unless they are transferring to another CNATRA, NFDS/Blue Angels or NATRACOM site, all accounts are suspended and after the required timeframe, deleted. The TRAWING IMSO at the last NATRACOM training wing and last phase of training should collect and destroy the CAC card prior to the IMS flight student's final

departure. An IMS flight student will not retain the CAC as a souvenir.

c. Monitoring and Acceptable Behavior

(1) All IMP and IMS are held to the same standards as U.S. personnel in regards to the acceptable use and behavior on any NATRACOM IS, reference (b). With the use of the SAAR-N and applicable training, all International Military personnel are briefed on what is acceptable usage and behavior and they are subject to monitoring.

(2) At no time, will IMP copy proprietary data from a Government computer onto any type of media (flash-drive, CD, DVD, HD, etc.), or onto a personal laptop for work outside of the work area, to a home, or any commercial cloud service unless authorized by the CNATRA ISSM in writing.

(3) Consistent with all users of DOD/DON IT assets, the visiting IMP and IMS will not attempt to download, install or run any application or program that is not already installed on the IS asset. Real-time monitoring tools are deployed to ensure that no unauthorized applications are installed. Reports are submitted to the CNATRA N6 Incident Management Team and actions of this sort will result in access privilege suspension until investigation actions are completed.

6. Responsibility. CNATRA CIO is the official approval authority for N6, which includes operations and support of IS for CNATRA, NFDS/Blue Angels and NATRACOM units. All support actions and documentations relative to IS administration will be channeled and coordinated through the respective chain of command, the IAO, IT Point of Contact (ITPOC), then to the CNATRA CIO office. Unit Commanding Officer (CO) will implement these policies, administration, guidelines and procedures within their commands.

7. Contact Information for CNATRA CIO: CNATRA (N6), 9035 Ocean Drive, Suite 322, Corpus Christi, TX 78419, DSN 861-3213 or Commercial (361) 961-3213.

D. M. EDGECOMB
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

WEB LINKS TO REFERENCES

Note: If clicking the link does not work, try copying the link and pasting it into the web browser.

CNATRAINST 5200.9A, Chief of Naval Air Training Command Information Officer Responsibilities, Functions, Relationships and Authorities
https://www.cnatra.navy.mil/pubs-instructions.asp

CNATRAINST 5239.3A, CNATRA Cybersecurity Program
https://www.cnatra.navy.mil/pubs-instructions.asp

CJCSM 6510.01B Cyber Incident Handling Program
http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

DOD 5220.22-M National Industry Security Program
http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

DODD 3020.40 DoD Policy and Responsibilities for Critical Infrastructure
http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf

DODD 5230.20 Visits and Assignments of Foreign Nationals
http://www.dtic.mil/whs/directives/corres/pdf/523020p.pdf

DODI 8500.01 Cybersecurity
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DODI 5200.02 DoD Personnel Security Program
http://www.cac.mil/docs/DODI-5200.02.pdf

DODI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DODM 5200.1, V3 DoD Information Security Program: Protection of Classified Information
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

OPNAVINST 5239.1C Navy Information Assurance (IA) Program
https://fas.org/irp/doddir/navy/opnavinst/5239_1c.pdf

SECNAVINST 4950.4B Joint Security Cooperation Education and Training
http://www.apd.army.mil/pdffiles/r12_15.pdf

SECNAVINST 5239.3B Department of the Navy Information Assurance Policy
https://fas.org/irp/doddir/navy/secnavinst/5239_3b.pdf

SECNAVINST 5510.30B Department of the Navy (DON) Personnel Security Program (PSP)
http://www.secnav.navy.mil/dusnp/Security/Personnel/Documents/SECNAVINST%205510.30B.pdf

SECNAVINST 5510.36A Department of the Navy (DON) Information Security Program (ISP)
http://www.secnav.navy.mil/dusnp/Security/Information/Documents/SECNAVINST%205510.36A.pdf

SECNAVINST 5510.34A Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
https://doni.daps.dla.mil/SECNAV%20Manuals1/Foreign%20Disclosure%20Manual%20CH%201.pdf

OPNAV-5239-14-SAAR-N

E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM0500-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID | DATE (DD/MM/YYYY):

SYSTEM NAME (Platform or Application): | LOCATION (Physical Location of System):

PART I *(To be completed by Requester)*

1. NAME (Last, First, Middle Initial): | 2. ORGANIZATION:

3. OFFICE SYMBOL/DEPARTMENT: | 4. PHONE (DSN and Commercial): DSN: COM:

5. OFFICIAL E-MAIL ADDRESS: | 6. JOB TITLE AND GRADE/RANK:

7. OFFICIAL MAILING ADDRESS: | 8. CITIZENSHIP: ☐ US ☐ FN ☐ LN ☐ Other | 9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS *(Complete as required for user or functional level access.)*:
☐ I have completed Annual IA Awareness Training. DATE (DD/MM/YYYY):

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS:

12. TYPE OF ACCESS REQUIRED: ☐ AUTHORIZED ☐ PRIVILEGED | 12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form. | DATE SIGNED (DD/MM/YYYY):

13. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED (Specify Category): ☐ OTHER:

14. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested. ☐ | 14a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date):

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT: | 15a. SUPERVISOR'S E-MAIL ADDRESS: | 15b. PHONE NUMBER:

16. SUPERVISOR'S NAME (Print Name): | 16a. SUPERVISOR'S SIGNATURE | 16b. DATE (DD/MM/YYYY):

17. SIGNATURE OF INFORMATION OWNER/OPR: | 17a. PHONE NUMBER: | 17b. DATE (DD/MM/YYYY):

18. SIGNATURE OF IAM OR APPOINTEE: | 19. ORGANIZATION/DEPARTMENT: | 20. PHONE NUMBER: | 21. DATE (DD/MM/YYYY):

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED

E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

22. **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 device 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.
- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

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 authentication at 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 by the 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 information system.
- 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.

E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

(Block 22 Cont)

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, Proxy Servers, 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 from the 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).

23. NAME *(Last, First, Middle Initial)*:	24. USER SIGNATURE:	25. DATE SIGNED *(DDMMMYYYY)*:
	SIGN HERE	

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

26. TYPE OF INVESTIGATION:	26a. DATE OF INVESTIGATION *(DDMMMYYYY)*:
26b. CLEARANCE LEVEL:	**26c. IT LEVEL DESIGNATION**
	☐ LEVEL I ☐ LEVEL II ☐ LEVEL III

27. VERIFIED BY *(Print name)*:	28. SECURITY MANAGER TELEPHONE NUMBER:	29. SECURITY MANAGER SIGNATURE:	30. DATE *(DDMMMYYYY)*:
		SIGN HERE	

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

31. TITLE:	31a. SYSTEM:	31b. ACCOUNT CODE:
	31c. DOMAIN:	
	31d. SERVER:	
	31e. APPLICATION:	
	31f. DATASETS:	
	31g. DIRECTORIES:	
	31h. FILES:	
32. DATE PROCESSED *(DDMMMYYYY)*:	32a. PROCESSED BY:	32b. DATE *(DDMMMYYYY)*:
	SIGN HERE	
33. DATE REVALIDATED *(DDMMMYYYY)*:	33a. REVALIDATED BY:	33b. DATE *(DDMMMYYYY)*:
	SIGN HERE	

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED

Page 3 of 4

Enclosure (2)

E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

INSTRUCTIONS

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

(1) Name. The last name, first name, and middle initial of the user.
(2) Organization. The user's current organization (i.e., USS xx, DoD,and government agency or commercial firm).
(3) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
(4) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
(5) Official E-mail Address. The user's official e-mail address.
(6) 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.
(7) Official Mailing Address. The user's official mailing address.
(8) Citizenship (United States (US), Foreign National (FN), Local National (LN), or Other), Identify appropriate citizenship in accordance with (IAW) SECNAV M-5510.30.
(9) Designation of Person (Military, Civilian, Contractor).
(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date of completion.

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

(11) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
(12) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters or settings.)
(12a) If Block 12 is Privileged, user must sign a Privilege Access Agreement form. Enter date of when Privilege Access Agreement (PAA) form was signed. Users can obtain a PAA form from the Information Assurance Manager (IAM) or Appointee.
(13) User Requires Access To. Place an "X" in the appropriate box. Specify category.
(14) Verification of Need to Know. To verify that the user requires access as requested.
(14a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
(15) Supervisor's Organization/Department. Supervisor's organization and department.
(15a) Official E-mail Address. Supervisor's e-mail address.
(15b) Phone Number. Supervisor's telephone number.
(16) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
(16a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
(16b) Date. Date supervisor signs the form.
(17) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
(17a) Phone Number. Functional appointee telephone number.
(17b) Date. The date the functional appointee signs the OPNAV 5239/14.
(18) Signature of Information Assurance Manager (IAM) or Appointee. Signature of the IAM or Appointee of the office responsible for approving access to the system being requested.
(19) Organization/Department. IAM's organization and department.
(20) Phone Number. IAM's telephone number.
(21) Date. The date the IAM signs the OPNAV 5239/14 form.
(22) Standard Mandatory Notice and Consent Provision and User Responsibilities. These items are in accordance with DoD Memo dtd May 9, 2008 (Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement) and DON CIO message Responsible and Effective Use of Dept of Navy Information Technology Resources" DTG 161108Z JUL 05.
(23) Name. The last name, first name, and middle initial of the user.
(24) User Signature. User must sign the OPNAV 5239/14 with the understanding that they are responsible and accountable for their password and access to the system(s). User shall digitally sign form. Pen and ink signature is acceptable for users that do not have a Common Access Card (CAC) or the ability to digitally sign the form.
(25) Date. Date signed.

C. PART III: Certification of Background Investigation or Clearance.

(26) Type of Investigation. The user's last type of background investigation (i.e., National Agency Check (NAC), National Agency Check with Inquiries (NACI), or Single Scope Background Investigation (SSBI)).
(26a) Date of Investigation. Date of last investigation.
(26b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(26c) Identify the user's IT designation level. If Block 12 is designated as "Authorized" then IT Level Designation is "Level III". If Block 12 is designated as "Privileged" then IT Level Designation is "Level I or II" based on SECNAV M-5510.30 dtd June 2006.
(27) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(28) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
(29) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
(30) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the functional activity or the customer with approval from OPNAV. This information will specifically identify the access required by the user.

(31 - 33b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If the completed form is transmitted electronically, the e-mail must be digitally signed and encrypted.

FILING: Form is purposed to use digital signatures. Digitally signed forms must be stored electronically to retain non-repudiation of electronic signature. If pen and ink signature must be applied, original signed form must be retained. Retention of this form shall be IAW SECNAV Manual M-5210.1, Records Management Manual. Form may be maintained by the Navy, the user's IAM, and/or Security Manager. Completed forms contain Personal Identifiable Information (PII) and must be protected as such.

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE

Page 4 of 4

FOR OFFICIAL USE ONLY WHEN FILLED

Enclosure (2)