



DEPARTMENT OF THE NAVY
COMMANDER
TRAINING AIR WING FIVE
7480 USS ENTERPRISE STREET SUITE 205
MILTON, FLORIDA 32570-6017

IN REPLY REFER TO

COMTRAWINGFIVEINST 5230.1D
N6
8 Nov 12

COMTRAWING FIVE INSTRUCTION 5230.1D

From: Commander, Training Air Wing FIVE

Subj: MANAGEMENT INFORMATION SYSTEMS (MIS) OPERATIONS, SECURITY, AND
ADMINISTRATION

Ref: (a) CNATRINST 5000.2C
(b) CNATRINST 5200.7B
(c) CNATRINST 5230.2A
(d) CNATRINST 5230.3A
(e) CNATRINST 5230.4A
(f) CNATRINST 5230.5A
(g) CNATRINST 5231.3A
(h) CNATRINST 5231.4A

Encl: (1) Training Air Wing FIVE Information Systems Security Policy

1. Purpose

a. To establish Training Air Wing (TRAWING) FIVE policies and guidelines to conform to Chief of Naval Air Training (CNATRA) Information Systems (IS) Security, Information Management (IM), and Information Technology (IT) directives.

b. To establish TRAWING FIVE Information Systems Security (ISP) Policy.

c. To delineate the procedures and responsibilities for the management, accountability, and the acquisition of resources supporting TRAWING FIVE's management information systems.

2. Cancellation. COMTRAWINGFIVEINST 5230.1C.

3. Scope. This instruction is applicable to all organizations within the purview of TRAWING FIVE who utilize and operate management information systems. This includes information systems hardware, software, data, and the supportive infrastructure within TRAWING FIVE departments, CNATRA detachment, and Training Squadrons. DoD/DoN Military and civilians, federal contractors, and Foreign Military Service personnel who have been granted access to government owned or controlled management information systems, whether processing sensitive information and/or unclassified For Official Use Only information are subject to the provisions herein.

4. Policy. TRAWING FIVE Management Information Systems personnel are responsible for the execution of appropriate IS policies and directives outlined in references (a) through (h), and serve as the central point of contact for all TRAWING FIVE Management Information Systems and subsequent IT/IM issues. The security of MIS resources is critical to mission accomplishment, thereby all TRAWING FIVE assets are assigned to Mission Assurance Category III (MAC III). MAC III systems handle information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

a. Procurement. All IT, IM and IS hardware and software shall be procured following the policies and guidelines outlined in reference (a).

b. Accountability. All IS equipment purchased and/or received, regardless of the method of acquisition will be reported to TRAWING FIVE Plant/Minor Property Clerk in accordance with references (g) and (h). Lifecycle management process will ensure the IT/IM/IS equipment is supported throughout its usage and properly identified for disposal when it no longer meets mission needs.

c. Supplies. All consumable supplies supporting the MIS and its mission will be borne by the user, squadron, department and/or detachment.

d. IS Asset Relocation and Disposition

(1) Legacy (Non-NMCI) assets are procured and/or acquired in support of TRANET computers, which hosts the Training Integrated Management Systems (TIMS) application. Under no circumstances should a user remove or relocate an IT asset without prior authorization by the CNATRA Information Technology Point of Contact (ITPOC). CNATRA CIO (N61) is responsible for the lifecycle management of all assets supporting legacy MIS.

(2) Navy/Marine Corps Intranet (NMCI) resources are government leased assets, purchased and supported through a services contract. The TRAWING FIVE/CNATRA ITPOC is solely responsible for the management and oversight of all leased NMCI assets and contract execution in support of TRAWING FIVE mission requirements. Due to the fiscal implications of this services contract, the ITPOC shall be the central point of contact for any changes in TRAWING FIVE NMCI requirements.

5. Action. The Commander, Naval Network Warfare Command (NETWARCOM) is the Navy Designated Approval Authority (DAA) for the NMCI Enterprise Network. CNATRA is the DAA for the TIMS application and NETC Training Network (TRANET) resources hosting this application. Commander TRAWING FIVE has been delegated authority and responsibility for the security, management, and administration of systems, applications, and networks supporting the Command's administrative and training missions. COMTRAWING FIVE staff shall execute the policies and directives as prescribed in reference (a-h), ensuring management information systems operated, maintained and administered comply with national, DoD and DoN policies.

a. Information Assurance Officer (IAO). The TRAWING FIVE IAO shall be designated in writing as the command's IAO. The IAO duties will include, but not limited to the following activities:

(1) Serves as the primary technical Information Assurance (IA) advisor, reporting to and advising the CNATRA IAM on all IA issues for management information systems and networks within TRAWING FIVE.

(2) Provides organizational level oversight and IA guidance in the implementation of the IA program for TRAWING FIVE and Training Squadrons IAW CNATRA policies and procedures.

(3) Act as the primary command liaison and assist CNATRA IAM with all matters, actions and efforts required to ensure compliance of all Information Systems Security and IA directives.

(4) Provide oversight to ensure the DoN Security Program is adhered to and implemented by all TRAWING FIVE commands, detachments, and activities.

b. TIMS Functional Administrator (TFA). The TRAWING FIVE TFA is responsible for TIMS administration and training requirements in support of the flight training mission. The TFA responsibilities include but not limited to the following:

(1) Provide organizational level oversight for all TIMS related issues for TRAWING FIVE and Training Squadrons.

(2) Head the TRAWING FIVE TIMS Process Action Team which shall include representation from each Training Squadron, Instructor Training Units, Academic Training and other stakeholders as necessary.

(3) Develop local policies for the identification and reporting of TIMS change requests.

c. Information Technology Point of Contact (ITPOC). The ITPOC provides IT customer support to NATRACOM commands and reports directly to CNATRA Deputy Contract Technical Representative on all respective funding, resource, and mission support capabilities for TRAWING FIVE

and Training Squadrons. The ITPOC responsibilities include but not limited to the following:

(1) Serves as the resident expert in NMCI contract products, services, and service level agreements.

(2) Responsible for NMCI asset management which includes all hardware, software and peripherals inventory, tracking and accountability process.

(3) Validates new requirements, process order modifications, submission of Move, Add, Change requests, and the certification of monthly service offerings through the invoice validation process.

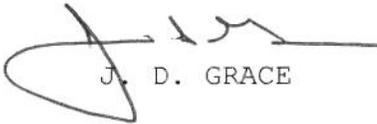
d. Information Assurance Security Officer (IASO). TRAWING FIVE Squadrons will designate, in writing an IASO. The IASO duties will include, but not limited to the following activities:

(1) Provide management oversight on all relevant IA and Computer Security initiatives for the squadron to include periodic computer asset inventory and user IA training.

(2) Serves as the squadron's central point of contact on all NMCI and legacy computer support initiatives impacting current and future mission capabilities.

(3) Provide assistance as needed in the establishment of NMCI and TRANET accounts for students and staff, identification of NAS Whiting Share Drive permissions for newly reported personnel, NMCI Public Folder access, permissions and data maintenance actions.

6. TRAWING FIVE Security Policy. All military, civilian, and contract personnel within the purview of TRAWING FIVE shall adhere to the Information Systems Security (ISP) Policy as delineated in enclosure (1).


J. D. GRACE

Distribution:
COMTRAWINGFIVEINST 5216.1S
Lists I, II, III

Commander, Training Air Wing FIVE

MANAGEMENT INFORMATION SYSTEMS SECURITY POLICY (ISP)



Commander, Training Air Wing FIVE
7480 USS Enterprise Street
Milton, Florida 32570

July 2011

Enclosure (1)

Subj: TRAINING AIR WING FIVE INFORMATION SYSTEMS SECURITY POLICY

Ref: (a) U.S. Navy Public Affairs Regulations
(b) SECNAVINST 5211.5E
(c) SECNAVINST 5239.3B
(d) SECNAVINST 5510.36A
(e) DoD Directive 8500.1
(f) DoD Directive 8500.2

Encl: (1) OPNAV Form 5239/14 System Authorization Access Request
(SAAR-N End User Agreement)
(2) CNATRA N6 NMCI-TRANET Account Request Form
(3) CNATRA N6 NMCI-TRANET Account Checkout Form
(4) Information Technology Acquisition Paper (ITAP)
(5) CNATRA Funding Request (CFR)

1. Purpose. The primary purpose of NMCI and NETC Training Community of Interest (COI) (TRANET) management information system and resources is to enhance the mission readiness of each command and subordinate units. These resources include the various microcomputers, networks and network workstations, network servers, and peripheral equipment that are used in support of the training mission. All personnel are expected to use computer resources responsibly, ethically, and lawfully in pursuit of TRAWING FIVE related functions.

2. Scope. This policy applies to all organizational components of TRAWING FIVE. The policies, guidance, and procedures established by this instruction support the national, Department of Defense, and Department of the Navy information system security requirements in accordance with references (a) through (f).

3. Objective.

a. To establish procedures for all aspects of information system security within COMTRAWING Five command including hardware, software, personal security, data, and administrative/operating procedures.

b. To establish an information system security program responsive to the needs of COMTRAWING FIVE management information systems and supportive mission objectives.

c. To establish procedures and provide guidance to ensure all information system software, hardware, and data are handled within the command are adequately protected against inadvertent disclosure, compromise, accidental or intentional destruction, unauthorized modification and loss, and to protect against denial of authorized user's access as a result of misuse or malicious acts, sabotage, or fraud.

d. Provide guidance for the implementation of a comprehensive security training program for all command information system users.

(1) All personnel reporting to TRAWING FIVE or subordinate Training Squadrons will check-in with the IAO. Upon completion of all IA documentation to include IA Training (IAA Ver.X and PII dated within one year), NMCI and/or TRANET accounts will be requested and established for system access through the ITPOC office by the IAO. OPNAV Form 5239/14 (SAAR-N), exhibits (1) and (2) will serve as the primary documentation in support of granting user system access and exhibit (3) will serve as the primary documentation provided by the squadron ITO for personnel detaching for check-out purposes for NMCI-TRANET account disable-deactivations.

(2) All management information system users will conform to the basic guidelines identified in the OPNAV Form 5239/14 (SAAR-N) User Responsibilities when utilizing systems and resources.

(3) Violations of the OPNAV Form 5239/14 (SAAR-N) User Responsibilities will result in system access suspension.

(4) IA Training is a requirement for all personnel administering, operating, and managing informational systems and resources in accordance with references (e) and (f). Annual computer based IA training meets this requirement for the vast majority of users. In addition, all personnel having roles and responsibilities beyond the basic user will have the appropriate training based on their assigned duties. At a minimum, all personnel accessing information systems will complete IAA Ver.X and PII training annually.

(5) As the importance of IT to our Naval war fighting team has increased, so has our reliance upon IT. This increased reliance demands that we protect the information and information systems we use. Additionally, we are each responsible for using IT resources in an effective, efficient, ethical, and legal manner. IM, IT, IS includes, but is not limited to, the following: Cell Phones, Blackberry, Personal Digital Assistants, Facsimile Machines, Internet access, radios, Electronic mail, telephones, computers, information and communication systems. Below are examples of effective and secure use of IT resources:

(a) Use consistent with the mission of TRAWING FIVE.

(b) Use For Official Use and authorized purposes only.

(c) Use related to administrative or other support activities considered consistent with the mission of TRAWING FIVE.

(6) The following are examples of unacceptable use of management information systems that will impact integrity and security of IS equipment and resources:

(a) Use of TRAWING FIVE computers or networks that violates federal, state, or local laws or statutes.

(b) Providing, assisting in, or gaining unauthorized or inappropriate access to TRAWING FIVE computing resources.

(c) Use of TRAWING FIVE computers or networks for unauthorized or inappropriate access to systems, software, or data at other sites.

(d) Activities that interfere with the ability to use TRAWING FIVE computing resources or other network connected services effectively.

(e) Dissemination of obscene, abusive, or other inappropriate e-mail that condones illegal or behavior not appropriate for good order or discipline.

(7) Department of the Navy guidance dictates all supportive NMCI IT/IM resources shall be purchased directly through the NMCI Services Contract through CNATRA N6.

(a) The CNATRA Wing ITPOC is directly responsible for adhering to and enforcing this directive for NMCI IT acquisitions.

(b) NMCI/Legacy computer and any supportive resource requirements must be submitted for approval to CNATRA CIO utilizing exhibits (4) and (5) through the CNATRA Wing ITPOC.

(c) TRAWING FIVE activities shall not utilize their assigned OPTAR funding for the procurement of IT/IM resources without the expressed consent and approval from CNATRA CIO.

(8) All IT/IM equipment and resources, whether in support of legacy or NMCI, will be accountable throughout its lifecycle. At a minimum, a 100 percent inventory of all items will be conducted on a semi-annual basis.

(9) All IT/IM equipment will be surveyed upon the completion of its lifecycle when either replaced or deemed to not meet mission requirements. The preferred method of equipment disposition will be through the Defense Re-utilization Management Organization (DMRO) process.

4. Action. The Commander, Naval Network Warfare Command (NETWARCOM) is the Navy Designated Approval Authority (DAA) for the NMCI Enterprise Network. The Commander, CNATRA is the DAA for the TIMS application and NETC Training Network (TRANET) resources hosting this application. Commander TRAWING FIVE has been delegated authority and responsibility for the security, management, and administration of systems, applications, and networks supporting the Command's administrative and training missions. COMTRAWING FIVE staff shall execute the policies and directives as prescribed in reference (a-h), ensuring management information systems operated, maintained and administered comply with national, DoD and DoN policies.

a. Information Assurance Officer (IAO). The TRAWING FIVE IAO shall be designated in writing as the command's IAO. The IAO duties will include, but not limited to the following activities:

(1) Serves as the primary technical Information Assurance (IA) advisor, reporting to and advising the CNATRA IAM on all IA issues for management information systems and networks within TRAWING FIVE.

(2) Provides organizational level oversight and IA guidance in the implementation of the IA program for TRAWING FIVE and Training Squadrons IAW CNATRA policies and procedures.

(3) Act as the primary command liaison and assist CNATRA IAM with all matters, actions and efforts required to ensure compliance of all Information Systems Security and IA directives.

(4) Provide oversight to ensure the DoN Security Program is adhered to and implemented by all TRAWING FIVE commands, detachments, and activities.

(5) Respond to IA incidents IAW established CNATRA IA guidelines and procedures.

(6) Receive, process, distribute, and store all inbound personnel's required documentation for obtaining access to TRAWING FIVE information systems.

b. TIMS Functional Administrator (TFA). The TRAWING FIVE TFA is responsible for TIMS administration and training requirements in support of the flight training mission. The TFA responsibilities include but not limited to the following:

(1) Provide organizational level oversight for all TIMS related issues for TRAWING FIVE and Training Squadrons.

(2) Liaisons with higher headquarters, adjacent echelon commands, and local personnel for all hardware and software configuration management requirements related to TIMS.

(3) Develop local policies for the identification and reporting of TIMS change requests.

c. Information Technology Point of Contact (ITPOC). The ITPOC provides IT customer support to NATRACOM commands and reports directly to CNATRA Deputy Contract Technical Representative on all respective funding, resource, and mission support capabilities for TRAWING FIVE and Training Squadrons. The ITPOC responsibilities include but not limited to the following:

(1) Serves as the resident expert in NMCI contract products, services, and service level agreements.

(2) Responsible for NMCI asset management which includes all hardware, software and peripherals inventory, tracking and accountability process.

(3) Validates new requirements, process order modifications, submission of Move, Add, Change requests, and the certification of monthly service offerings through the invoice validation process.

d. Information Assurance Security Officer (IASO). TRAWING FIVE Squadrons will designate, in writing an IASO. The IASO duties will include, but not limited to the following activities:

(1) Provide management oversight on all relevant IA and Computer Security initiatives for the squadron to end user IA training.

(2) Serves as the squadron's central point of contact on all NMCI and legacy security initiatives impacting current and future mission capabilities.

(3) Provide assistance as needed in the establishment of NMCI and TRANET accounts for students and staff, identification of NAS Whiting Share Drive permissions for newly reported personnel, NMCI Public Folder access, permissions and data maintenance actions.

(4) Act as a "First responder" to unit IA incidents for such things as network cable removal and posting of "Do not use" signs to mitigate further risks to the network and systems. Ensures the IAO is notified of any IA incidents using the most expedient means available.

(5) Attend IAO provided IA training at least quarterly to refresh and expand information systems security knowledge and awareness.

e. Information Technology Officer (ITO). TRAWING FIVE Squadrons will designate, in writing, an ITO. The ITO duties will include, but are not limited to, the following activities:

(1) Serves as the squadron contact for all user account move add, change (MAC) requests.

(2) Serves as the squadron contact for all hardware, software move, add, change (MAC) requests.

(3) Serves as primary contact for all semi-annual inventory process ensuring access to all required hardware.

(4) Serves as the primary point of contact for dissemination of relevant NMCI-TRANET information provided by the ITPOC.

5. TRAWING FIVE Security Policy. All military, civilian, and contract personnel within the purview of TRAWING FIVE shall adhere to the Information Systems Security (ISP) Policy as delineated in enclosure (1).

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:
 - o 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.
 - o At any time, the U.S. Government may inspect and seize data stored on this information system.
 - o 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.
 - o 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.
 - o 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.
 - o 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.
 - o 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.

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 (DDMMYYYY): |
|---|---------------------|-----------------------------|

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

| | | | |
|-------------------------------|--|---------------------------------|----------------------|
| 26. TYPE OF INVESTIGATION | 26a. DATE OF INVESTIGATION (DDMMYYYY): | | |
| 26b. CLEARANCE LEVEL: | 26c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III | | |
| 27. VERIFIED BY (Print name): | 28. SECURITY MANAGER TELEPHONE NUMBER: | 29. SECURITY MANAGER SIGNATURE: | 30. DATE (DDMMYYYY): |

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

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

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 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.
- (15a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (15b) Date. Date supervisor signs the form.
- (16) Supervisor's Organization/Department. Supervisor's organization and department.
- (16a) Official E-mail Address. Supervisor's e-mail address.
- (16b) Phone Number. Supervisor's telephone number.
- (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.

INFORMATION TECHNOLOGY ACQUISITION PAPER (ITAP)

CNATRA #:

Date of submission:

FROM UNIT:

POC Name:

POC Title:

POC PHONE:

POC E-MAIL:

INFORMATION TECHNOLOGY TO BE ACQUIRED

REQUIREMENT SHORT TITLE AND DESCRIPTION OF MISSION NEED:

CURRENT SUPPORT:

IMPACT OF PROCUREMENT OR NON-PROCUREMENT:

(Provide tangible or non-tangible benefits)

SUBMITTING UNIT SIGNATURES

Submitted by: _____

Program Manager **Date**

Functional Requirements Validated by: _____

Commanding Officer/Dept Head **Date**

IT Functional Area _____

Local Unit IMIT POC **Date**

Resources Management Funds Available _____

Resources Management Head **Date**

YES / NO

IT COSTS (USER WILL LEAVE SECTION BLANK)-CNATRA CIO ACTR ACTION

| INFORMATION TECHNOLOGY | TYPE | QTY | ESTIMATED COSTS |
|----------------------------|------|-----|-----------------|
| EQUIPMENT: | | | |
| SOFTWARE : | | | |
| SERVICES: | | | |
| SUPPORT SERVICES: | | | |
| TOTAL IT COSTS: | | | |
| TOTAL COSTS OTHER THAN IT: | | | |
| TOTAL ACQUISITION COSTS: | | | |

OTHER ALTERNATIVES CONSIDERED:

FUNDING: (IDENTIFY UNIT FUNDING CITE
SOURCE)

ACQUISITION STRATEGY:

PROJECTED ISSUE DATE:

COMPETITIVE/OTHER:

IT ACQUISITION LIFE CYCLE:

IT ACQUISITION TYPE:

LIST OF USING ORGANIZATIONS OR USERS:

RISK ASSESSMENT:

INTERFACE CONSIDERATIONS:
TRANSITION STRATEGY:

ARCHITECTURE COMPLIANCE:

OTHER COMMENTS: (USE ADDITIONAL
SHEETS, IF NEEDED)

CNATRA COMMAND INFORMATION OFFICER (CIO)

Date

Approved

Disapproved

Reason for disapproval

CNATRA FUNDING REQUEST

| PART I: COMPLETED BY THE REQUESTOR | | | |
|---|---|--|---|
| Name /Phone Number | Department | Date (mm/dd/yyyy) | Request # |
| | | | |
| Amount Needed | Priority | Date Required | <input type="checkbox"/> New Requirement <input type="checkbox"/> Increase to Existing Requirement |
| | | | |
| Describe the requirement and why it is needed (Check one: <input type="checkbox"/> One-time <input type="checkbox"/> Recurring) | | | |
| | | | |
| Describe what happens if not funded (consequences and impact) | | | |
| | | | |
| PART II: FINANCIAL REVIEW | | | |
| Status of Request: (click to select) | <input type="checkbox"/> Approved <input type="checkbox"/> Disapproved | <input type="checkbox"/> Pending <input type="checkbox"/> Other | Review Date |
| Comments | | Priority | |
| | | | |
| Approved by: | Signature | | |
| | | | |
| PART III: COMPLETED BY CNATRA N8 | | | |
| Job Order Number | Expense Element | Document Type: (click to select) | <input type="checkbox"/> 2276 <input type="checkbox"/> 2275 <input type="checkbox"/> MIPR <input type="checkbox"/> Other |
| | | | |
| Approved by: | Signature | | |
| | | | |