

FOR OFFICIAL USE ONLY



DEPARTMENT OF THE NAVY

COMMANDER
NAVAL NETWORK WARFARE COMMAND
2465 GUADALCANAL ROAD SUITE 12
VIRGINIA BEACH VA 23459-3228

5239

Ser ODAA/0777

APR 06 2010

From: Commander, Naval Network Warfare Command

To: Commander, Navy Installation Command

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE
UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM
(PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND
INSTALLATIONS (FY10L0487)

- Ref:
- (a) OPNAV Instruction 5239.1C, Navy Information Assurance (IA) Program of 20 Aug 08
 - (b) DON CIO Washington DC 311917Z Mar 08 Department of the Navy's Transition Plan from DITSCAP to DIACAP
 - (c) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) of 28 Nov 07
 - (d) CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities of 9 Jul 08
 - (e) CJCSM 6510.01 CH-3, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND) of 25 Mar 03
 - (f) COMNAVNETWARCOM Norfolk VA 211600Z Dec 06 Navy Telecommunications Directive (NTD) 11-06, Promulgation of the System Identification Profile (SIP) for Navy IT Certification and Accreditation Process
 - (g) COMNAVNETWARCOM Norfolk VA 022152Z May 08 Announcement of the Sustainability and Supportability Document
 - (h) DoD Instruction 8500.2 Information Assurance (IA) Implementation of 6 Feb 03
 - (i) NAVCYBERDEFOPSCOM Norfolk VA 062305Z Mar 06 NCDOC Computer Tasking Order (CTO) 06-02 Directive for Automated Scanning and Remediation of Network Vulnerabilities
 - (j) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management of 15 Aug 04
 - (k) DoD 8570.01-M, Information Assurance Workforce Improvement Program of 19 Dec 05

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM (PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND INSTALLATIONS (FY10L0487)

- (l) OPNAV Navy-Marine Corps Unclassified Trusted Network Protection (UTNProtect) Policy, Ver 1.0 of 31 Oct 02 w/changes
- (m) DoD CIO Memo, Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media of 3 Jul 07
- (n) DON CIO Washington DC 081605Z Jan 09 DON Federal Information Security Management Act Goals for FY 2009
- (o) DON CIO Washington DC 181430Z May 09 Department of the Navy Privacy Impact Assessment (PIA) Guidance
- (p) DON CIO Washington DC 291600Z Feb 08 DON Contingency Plans and Testing Guidance
- (q) Defense Information Systems Agency (DISA) SIPRNET Global Information Grid (GIG) Interconnection Approval Process (GIAP) Connection Requirements of Oct 06
- (r) COMNAVNETWARCOM ltr 5239 Ser ODAA/1705, Navy ODAA Guidance Memorandum 02-07; Guidance for a Comprehensive Plan of Action and Milestones (POA&M) of 14 Jun 07
- (s) Information Assurance Tracking System (IATS) website <https://iats.nmci.navy.mil>, Reference # 16181

Encl: (1) Signed Certification and Accreditation (C&A) Package Signature Page
(2) Signed Contingency Plan Signature Page

1. By authority granted in reference (a), an ATO is hereby granted for the operation of the unclassified stand-alone PAS Version 2.1 aboard U.S. Navy Ships and Installations. This ATO serves as a Type Accreditation and requires installation and management per the approved configuration along with site installation Certification and Accreditation (C&A) documentation updates, and is granted in accordance with references (b) and (c), in compliance with references (d) through (r), and based on review of the information contained in reference (s). Enclosures (1) and (2) are approved. **This accreditation does not allow connection to any networks outside of the accreditation boundary.**

2. This ATO expires on **22 March 2013** or sooner if there are modifications that change the security posture of the stand-alone PAS Version 2.1. Changes must be submitted in writing

FOR OFFICIAL USE ONLY

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM (PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND INSTALLATIONS (FY10L0487)

through the Echelon II representative for Certification and Accreditation processing prior to implementation.

3. PAS is a smartcard compatible application developed to automatically establish and maintain accountability of individuals assigned access rights to a designated facility or ship. PAS generates reports that provide a current snapshot of those present and those departed from a ship or facility as well as archive reports of historical activity by date, event, person, and location. Individuals are registered in the application's database either manually, by reading demographic data stored on the Integrated Circuit Chip (ICC) of their Smartcard, or through the import of a comma separated value (*.csv) file.

4. The PAS Version 2.1 has been designated as Mission Assurance Category (MAC) Level II, and is authorized to process information at a confidentiality level of sensitive up to Unclassified FOUO in the System High mode of operation.

5. Reference (j) establishes policy to implement Information Assurance (IA) training, certification and workforce management programs for all DoD Component personnel. You are required to take appropriate action, in accordance with references (j) and (k), to ensure the identification and categorization of positions conducting IA functions. This includes ensuring that these individuals are trained and certified in order to professionalize personnel commensurate with their Information System (IS) user responsibilities and IA functions, and to document and track IA awareness training and certification status. IA training and certification requirements also apply to authorized contractor users and contractor personnel performing IA functions.

6. As per the certification determination letter dated 25 March 2010 and contained in reference (s), the overall risk was identified as **Low**. In order to retain this ATO, you are required to comply with all DoD and Navy policy requirements for IA and ensure the items listed below are accomplished. Non-compliance may result in termination of this ATO.

- a. Technical issues: None
- b. Non-technical issues:

FOR OFFICIAL USE ONLY

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM (PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND INSTALLATIONS (FY10L0487)

(1) The IA Controls listed below have been identified as "inherited" from the operational site. Prior to installation of the PAS Version 2.1 the operational site must validate that these IA Controls are compliant within the site's accreditation boundary. The Program Management Office (PMO) must be notified if any "inherited" IA Controls are found to be non-compliant or become non-compliant as a result of system implementation. If this system is installed with non-compliant IA Controls, the installation may invalidate the operational site's accreditation.

(2) Installation sites are required to check for PAS IAVA updates and ensure that Virus definition files are kept up-to-date via a DOD approved method and within required time periods. The IAM is required to document these actions.

List of Inherited IA Controls:

COBR-1	CODB-2	CODP-2	COEF-2	COMS-2	COPS-2
COSP-1	COSW-1	DCDS-1	DCHW-1	DCSD-1	DCSR-2
DCSS-2	EBBD-2	ECVP-1	PECF-1	PECS-1	PEDI-1
PEEL-2	PEFD-2	PEFI-1	PEFS-2	PEHC-2	PEMS-1
PEPF-1	PEPS-1	PESL-1	PESP-1	PESS-1	PETC-2
PETN-1	PEVC-1	PEVR-1	PRAS-1	PRMP-1	PRRB-1
PRTN-1	VIIR-1	VIVM-1			

c. Ensure implementation of personnel and non-technical security controls described in the DIP version 2.2 dated 2 March 2010 contained in reference (s).

d. Ensure implementation of the Information Assurance Vulnerability Management program required patches/fixes per reference (e).

e. Ensure identification and currency of the Information Assurance Manager associated with this system in the DIACAP Team Roles, Member Names and Contact Information section of the SIP reference (f).

f. Ensure annual testing of your site contingency plan per reference (e).

g. Ensure compliance with Navy firewall configuration guidance, as defined by reference (l).

FOR OFFICIAL USE ONLY

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM (PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND INSTALLATIONS (FY10L0487)

h. Ensure use of only those legacy applications that have been approved by the Functional Area Manager (FAM) and accredited by the Navy ODAA.

i. Ensure compliance with requirements for proper protection of data and systems, as defined by reference (h).

j. Ensure implementation of automated enterprise-wide vulnerability scanning, security patch remediation and compliance reporting tools on Navy NIPRNET and SIPRNET assets, as directed by reference (i).

k. Per reference (m), ensure all unclassified DoD data at rest that has not been cleared for public release and is stored on mobile computing devices or removable storage media is treated as sensitive data and encrypted using DoD approved encryption technology.

l. Reference (o) expanded the requirement to complete and submit a PIA (DoD Form 2930 Nov 2008) for all DON systems whether or not the system collects, maintains or disseminates Personally Identifiable Information (PII). IT systems with no PII will submit Section 1 of the PIA form, obtain local signatures and send to DON CIO. IT systems with PII must complete Sections 1 through 4 and submit to DON CIO for approval. Reference (o) contains guidance and procedures to submit an approved PIA or a Plan of Action and Milestones (POA&M) in lieu of an approved PIA as part of the system C&A package. Questions regarding DON PIA guidance and reporting should be submitted to the DON CIO Web site:
<http://www.doncio.navy.mil>.

m. Ensure a Supportability and Sustainability document is signed and submitted as per reference (g) and yearly thereafter as part of the annual requirements.

7. Reference (n) identifies DON goals to maintain 100% ATO or Interim ATO accreditation status of all systems requiring certification and accreditation, and maintain 100% compliance with FISMA required annual security reviews, annual testing of security controls, and annual evaluation of contingency plans. Each system must maintain compliance with required annual reviews, tests, and evaluations within the 12 month period of the last review cycle performed. You are required to take

FOR OFFICIAL USE ONLY

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE UNCLASSIFIED STAND-ALONE PERSONNEL ACCOUNTABILITY SYSTEM (PAS) VERSION 2.1 ABOARD U.S. NAVY SHIPS AND INSTALLATIONS (FY10L0487)

action to achieve DON FISMA accreditation and annual systems test, evaluation and review goals or be subject to DON non-compliance actions.

8. Consent to Monitor - In accordance with the requirements of reference (d), NAVNETWARCOM acknowledges that Defense Information Systems Agency (DISA) will conduct periodic monitoring of Navy networks. NAVNETWARCOM acknowledges and consents to DISA conducted assessments to include periodic, unannounced vulnerability assessments on connected host systems to determine effective security features and enhance IA posture.

9. POC: Ms. Marianne Chalut, Legacy Enterprise Security Lead or Darcee Branham, CTR, (757) 417-6719 ext. 0, Email: NNWC_ODAA@navy.mil.



T. M. JOHNSON
By direction

Copy to:
IATS Ref # 16181
CNIC CIO Washington DC

C&A PACKAGE SIGNATURE PAGE

This DIACAP Certification and Accreditation (C&A) Package documents the security requirements and conditions necessary for Accreditation of PAS 2.1. This C&A package is a living document that contains or references all information necessary to make an objective, management-level decision and represents an agreement among the PAS User Representatives, Program Manager (PM), Validator, Certification Authority (CA), and Designated Accrediting Authority (DAA) on the level of effort, security requirements, and policy required to certify and accredit PAS.

This document addresses certification requirements for a system accreditation as defined in the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The development of this PAS C&A package is to satisfy DIACAP requirements of the Department of Defense Instruction (DoDI) Memorandum 8510.bb, Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance Memorandum; Federal Information Security Management Act (FISMA); Department of Defense (DoD) Directive (DoDD) 8500.1; DoDI 8500.2; as well as to satisfy the Department of Navy (DON), Chief of Naval Operations (CNO), Information Assurance (IA) Publication (PUB) 5239-13 Volume III. The PAS C&A package is a living document and will be updated as the system development progresses and new information becomes available.

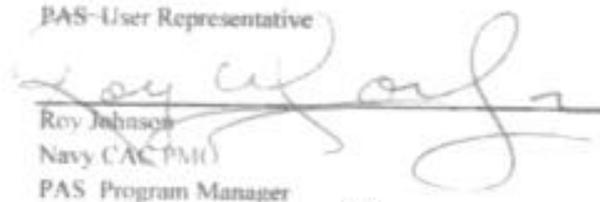
The undersigned concur with the information contained in this C&A package and agree that it accurately describes the security implemented for PAS. This agreement, in effect, certifies that the PAS meets the security requirements necessary for accreditation, operation up to and including the Unclassified (For Official Use Only level as described throughout this package.



Courtney Callin
Navy CAC PMO
PAS-User Representative

2-25-2010

Date



Roy Johnson
Navy CAC PMO
PAS Program Manager

2/25/2010

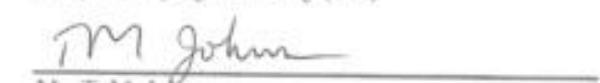
Date



Mr. Paul Hilton
COMSPAWARSYSCOM
Navy Certifying Authority (CA)

26 Mar 10

Date



Mr. T. M. Johnson
COMNAVNETWARCOM
Operational Designated Accrediting Authority (ODAA)

4/6/10

Date

ENCL (1)

**Approval & Agreement for the
Contingency Plan for Personnel Accountability System (PAS)**

DADMS Number: 76180

Information Technology (IT) systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Many "vulnerabilities" can be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort; however, it is virtually impossible to completely eliminate all risks.

Contingency planning will mitigate the risk of system and service unavailability by focusing on effective and efficient recovery solutions.

This contingency plan contains or references all information necessary to make an objective, management-level decision and represents an agreement among the operational Designated Accrediting Authority (DAA), Program Manager (PM), and the User Representative regarding the contingency plan for the Personnel Accountability System.

The undersigned concur with the information contained in this contingency plan and agree that it accurately describes the efforts to be implemented to maintain the operation of the Personnel Accountability System.

Courtney A. Callen
User Representative (Courtney Callen)

2 25 2010
Date

Ray Johnson
Program Manager (Ray Johnson), Navy Common Access
Card Program Manager

2/25/2010
Date

T.M. Johnson
Operational Designated Accrediting Authority (T. M.
Johnson), Commander, Naval Network Warfare Command

4/6/10
Date

ENCL(2)