



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

OPNAVINST 5239.3A
N2
18 January 2008

OPNAV INSTRUCTION 5239.3A

From: Chief of Naval Operations

Subj: NAVY IMPLEMENTATION OF DEPARTMENT OF DEFENSE INTELLIGENCE
INFORMATION SYSTEM (DODIIS) PUBLIC KEY INFRASTRUCTURE
(PKI)

Ref: (a) Director of Central Intelligence Directive (DCID)
6/3, 5 Jun 99
(b) DoD Instruction 8500.2, Information Assurance (IA)
Implementation, 6 Feb 03
(c) DODI 8520.2, Public Key Infrastructure (PKI) and
Public Key (PK) Enabling, 1 Apr 2004
(d) DODIIS Security Certification and Accreditation Guide,
Apr 01
(e) DODIIS-PKI Concept of Operations, 4 Mar 04
(f) DoD Sensitive Compartmented Information Administrative
Security Manual DoD 5105.21-M-1, Aug 98
(g) SECNAV M-5510.36, 30 Jun 06
(h) DODIIS-PKI Trusted Agent Handbook, 1 Aug 07

Encl: (1) Obtaining a User's DODIIS PKI Certificate

1. Purpose. This instruction:

a. Supports protection requirements for information systems used within the Intelligence Community (IC) as directed by references (a) and (b).

b. Directs the use of DoD Intelligence Information System (DODIIS) Public Key Infrastructure (PKI) as an Information Assurance (IA) protection safeguard within the Navy by all Navy Commands with access to the Joint World-Wide Intelligence Communications System (JWICS). Reference (c) directs the use of the DoD PKI as an IA protection safeguard within the Navy by all Navy Commands accessing the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) or SECRET Internet Protocol Router Network (SIPRNet).

18 January 2008

c. Assigns responsibilities for implementation of DODIIS PKI.

2. Cancellation. OPNAVINST 5239.3 is cancelled.

3. Applicability. This instruction applies to all Navy Commands with access to JWICS. Marine Corps personnel assigned to these commands will be supported in accordance with this instruction.

4. Background: The Director, Defense Intelligence Agency (DIA) is assigned by reference (a) the responsibility for JWICS IA through a Certification and Accreditation (C&A) process. The requirements of this process are detailed in reference (d). As part of the specific JWICS IA effort, DIA mandated DODIIS PKI use on JWICS in reference (e). All DoD personnel who require JWICS access must possess and use a DODIIS PKI certificate on their command's JWICS terminal in order to securely utilize the JWICS environment. Increasingly, JWICS applications are being Public Key Enabled (PKE), requiring users to hold a valid DODIIS PKI certificate to obtain specific information accessed through the PKE application. Enclosure (1) provides Department of the Navy (DON) JWICS users a general set of steps required to obtain a DODIIS PKI user certificate.

5. Scope. All Navy Commands with access to JWICS will implement the use of DODIIS PKI certificates for all users and equipment as specified in reference (d), and as amplified in this instruction.

6. Key Definitions

a. Public Key Infrastructure (PKI) - An enabling technology that enhances information systems security by providing a high degree of assurance of data confidentiality, integrity, authentication, and user identification among users of public key enabled information systems, including network login, e-mail, and web-based information services.

b. DODIIS Full Service Directory (FSD) - A directory of verified JWICS users that permits the issuance of a DODIIS PKI certificate. It is also the repository of JWICS user information, including their public key certificates. This directory is maintained by DIA. The Navy users are entered into the DODIIS FSD through the automated service directory, maintained by Ground Intelligence Support Activity (GISA), Fort Bragg, NC.

18 January 2008

c. Special Security Officer (SSO) - An active duty service member or DoD civilian at Navy commands handling SCI material, designated in writing by the Commanding Officer who is responsible for the security management, operation, implementation, use and dissemination of all Communications Intelligence and other types of SCI material within the command. Specific grade requirements for the SSO are detailed in reference (d).

d. Special Security Representative (SSR) - An active duty service member or DoD civilian at Navy commands handling Sensitive Compartmented Information (SCI) material, designated in writing by the Commanding Officer to assist the command's SSO in the security management, operation, implementation, use and dissemination of all Communications Intelligence and other types of SCI material within the command. Specific grade requirements for the SSR are detailed in reference (f).

e. Information Assurance Manager (IAM) - An active duty service member or DoD civilian at Navy commands, designated in writing by the Commanding Officer to be the point of contact for the command for all command IA matters and implements the command's IA program. Appointment of an IAM is required by reference (g).

f. Information Assurance Officer (IAO) - An active duty service member or DoD civilian at Navy commands, designated in writing by the Commanding Officer to be responsible for implementing and maintaining the command's information technology systems and network security requirements. An IAO is appointed for each information system and network in the command and is required by reference (g). The IAO supports the IAM.

g. Trusted Agent (TA) - An individual with JWICS access assigned in writing within a Navy command and locally trained to accomplish the task of verifying the identity (face-to-face) of a user requesting a DODIIS PKI certificate. After identity verification the TA can then provide the user with the one-time personal identification number (PIN) required for completion of the certificate application process. The duties and responsibilities of the TA are specified in reference (g). The command's SSO or SSR may also accomplish the user identification verification and issue the PIN.

h. User - A person assigned to a Navy command that has a requirement to access JWICS in the execution of duties and requires the issuance of a DODIIS PKI certificate.

7. Responsibilities

a. Office of the Chief of Naval Operations (OPNAV) N2, as the Navy's Senior Official of the Intelligence Community (SOIC):

(1) Coordinate the DON IA requirements for the DON SCI Intelligence program, and the DON portion of the DODIIS with DIA per reference (g).

(2) Promulgate DODIIS PKI policies within the Navy to support DIA IA policy and management of JWICS.

(3) Make recommendations to DIA and the Director of National Intelligence Chief Information Officer (DNI CIO) as necessary to incorporate Navy requirements for JWICS use.

(4) Maintain this instruction

b. Office of Naval Intelligence (ONI)

(1) Assist OPNAV N2 through the administration and management of the IA requirements for the DON SCI Intelligence Program, and the DON portion of DODIIS and provide recommendations for changes to SCI IA policy for discussion with DIA and ODNI CIO.

(2) Initiate and maintain appropriate service level agreements with the Army's GISA to host the Navy's FSD entries and all necessary support to access the DODIIS FSD.

(3) Incorporate DODIIS PKI certificate requirements in existing ONI training courses for SSO/SSRs and JWICS users to include procedures for obtaining a DODIIS PKI certificate and how to export a certificate for personnel being sent on temporary duty to another command.

(4) Provide DODIIS PKI training to the Office of the Chief of Naval Operations, COMUSFLTFORCOM/COMPACFLT, Numbered Fleets and regional Naval Commanders' staffs.

(5) Provide on-site DODIIS PKI training to other Navy commands in conjunction with other scheduled ONI visits or when requested.

(6) Publish and maintain on JWICS a Navy DODIIS website where DON SSOs and SSRs and users may obtain DODIIS PKI information.

(7) Publish and maintain a list of all Navy SSO/SSRs by command on the Navy DODIIS website.

(8) Task Regional Special Security Offices (SSO) and Information Systems Security Managers (ISSM) to:

(a) Review individual command implementation of DODIIS PKI certificates and use within their geographic area of responsibility and make available DODIIS PKI training materials developed by ONI as part of normal command visits.

(b) Identify DODIIS PKI certificate training discrepancies and refer them to the appropriate ONI points of contact for additional training. Regional SSO/ISSMs must ensure immediate corrective actions are taken against any issues that threaten the security of JWICS in accordance with this instruction and references (a), (b) and (d) through (h).

(c) Inspect DODIIS PKI certificate implementation and compliance for all commands within their geographic area of responsibility during normal security inspections or as directed by higher authorities.

c. COMUSFLTFORCOM/COMPACFLT

(1) Provide direction and assistance to the type commander's designated SSO/SSR as required to support fleet units DODIIS PKI requirements.

(2) Assist shore installations SSO/SSRs in the registration of users for DODIIS PKI certificates.

(3) Collect feedback and recommendations from fleet and shore commands regarding the DODIIS PKI requirements and provide to ONI for discussion with DIA by OPNAV N2.

(4) Issue written guidance to tailor procedures for use and issuance of DODIIS PKI, if necessary.

d. Type Commander

(1) Provide support to fleet units in registering new users for DODIIS PKI certificates when requested.

(2) Modify fleet unit pre-deployment checklists to include DODIIS PKI policy implementation in the training certification process and verify unit compliance with this instruction.

(3) Inspect fleet unit DODIIS PKI certification procedures as part of command inspections.

(4) Assist fleet units in obtaining DODIIS PKI certification training from ONI, if required.

e. Numbered Fleets/Regional Naval Commanders

(1) Support OCONUS shore installations within their AOR and deployed fleet unit requirements to register new users for DODIIS PKI certificates, if required.

(2) Assist OCONUS shore installations in obtaining DODIIS PKI certification training from ONI, if required.

f. All Afloat/Shore JWICS-Capable Commands

(1) Appoint a command SSO and SSR in writing, providing a copy of their appointment letters to GISA, Fort Bragg, NC, (Facsimile DSN: 239-2962, Commercial: 910-432-2962) and ONI (ONI-5, DSN: 659-4146, Commercial: 301-669-4146).

(2) Appoint command TAs in writing and ensure each TA completes all necessary training as specified in references (e) and (h).

(3) Ensure that the SSO/SSR/TAs fully comply with all requirements to authenticate an individual's identity prior to issuing the one-time PIN as required by reference (h) and develop site specific documentation and process to include an authentication checklist. Site specific documentation requirements for the authentication process may be accessed on JWICS at <http://www.dia.ic.gov/proj/dodiis/documentation>.

(4) Ensure that all assigned JWICS users and appropriate equipment are issued DODIIS PKI certificates, and ensure these certificates are maintained.

(5) Ensure the command IAM and JWICS IAO have incorporated the requirements for JWICS DODIIS PKI certificates into their documentation and assist the SSO/SSR in maintaining DODIIS PKI proficiency by all JWICS users.

(6) Maintain a command listing of all user and equipment DODIIS PKI certificates issued to include expiration date.

(7) Conduct annual DODIIS PKI training to all assigned users.

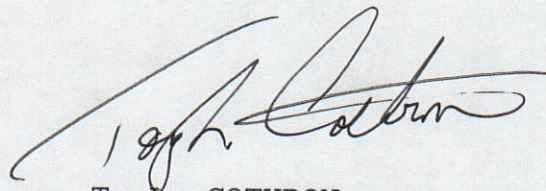
(8) Request DODIIS PKI training assistance from ONI or other sources as necessary to ensure user awareness and proficiency.

(9) Develop command procedures to address acceptance and installation of user certificates from other commands in the event of short-duration augmentation of personnel.

(10) Develop command procedures to ensure user certificates for command personnel are forwarded to other commands when personnel are being sent as short-duration augmentation assignments.

(11) Demonstrate DODIIS PKI certificate compliance as part of the type commander's training certification process, all security inspections and during command inspections.

(12) Execute pre-deployment checklists to minimize requirements for registering new users during deployment.

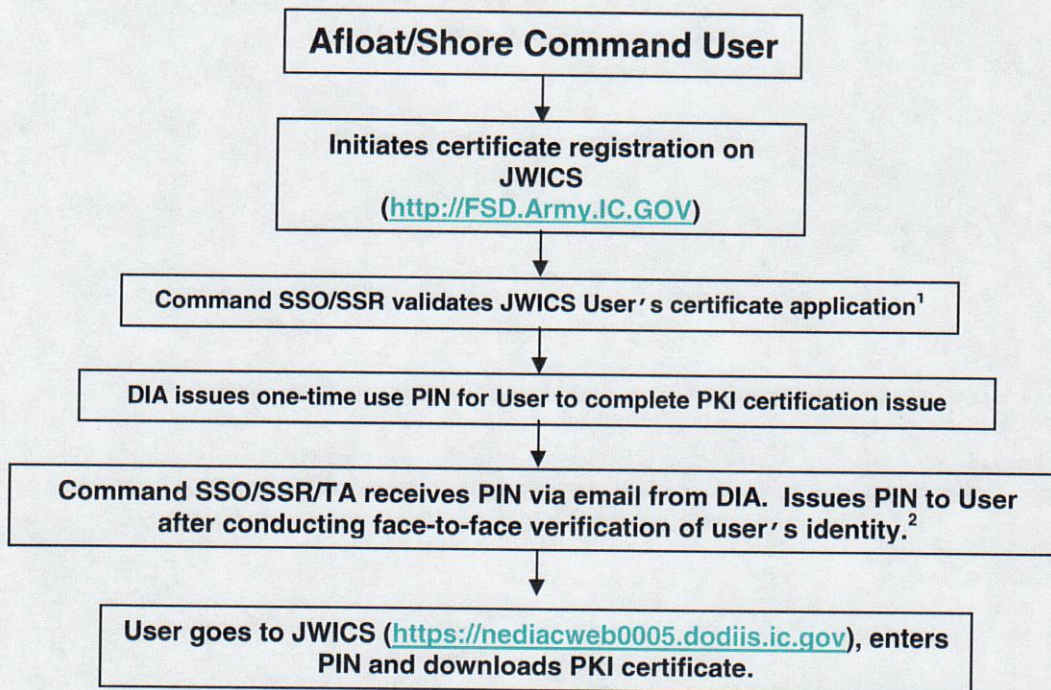


T. L. COTHRON
Director of Naval Intelligence

Distribution:

Electronic only, via Department of the Navy Issuances website
<http://doni.daps.dla.mil>

Obtaining a User's DODIIS PKI Certificate



¹SSO/SSR may also reject or cancel the registration. This diagram assumes neither of these actions is taken.

²Command may appoint in writing one or more Trusted Agents, if desired.