

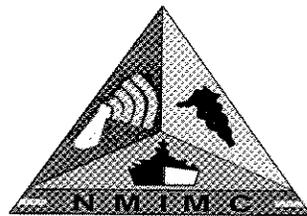
**NAVY MEDICINE**  
World Class Care...Anytime, Anywhere

---

# **Non-U.S. Citizen Access to Navy Medicine Information and Networks**

**Requirements and Process**

15 May 2007  
Version 1.0



Prepared by:

**Navy Medicine Information Management Center  
Code 03 Information Assurance Team  
8901 Wisconsin Ave, Bldg 27  
Bethesda, Maryland 20889-5605**

## EXECUTIVE SUMMARY

To prevent unauthorized access to sensitive information, all Department of Defense (DoD) employees that are to be assigned to National Security Positions require a background investigation (the extent of investigation will be dependent on the position sensitivity and access requirement). National Security Positions are defined as activities that support the U.S. Government and have access to information that can affect the protection of the nation from foreign aggression and espionage. Activities concerned with the preservation of U.S. military strength (e.g. DoD medical positions) are designated as National Security Positions.

Within the Department of the Navy (DON), sensitive duties (with or without IT responsibilities) have been designated as National Security Positions. DoD 5200.2-R DoD Personnel Security Program states that assignment to sensitive duties shall be granted only to U.S. citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the U.S., strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion.

To comply with DoD 5200.2-R the DON has established requirements to help mitigate the risk of attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. There are three sensitivity levels (IT-I, IT-II, and IT-III) for determining national security positions that apply equally to all DON contractors, consultants, and civilian employees.

Providers, system administrators, and file clerks employed at DON military treatment facilities have access to sensitive information; therefore, occupy IT-II positions and require U.S. citizenship. In those rare instances in which a qualified U.S. citizen is not available, a foreign national may be considered for a sensitive position **only after** authority to hire the individual has been granted by the CNO (N90N2) Personnel Security Branch. Temporary authority to hire non-U.S. personnel to national security / sensitive assignments or duties pending the results of security investigations may be granted **only by** CNO (N90N2) on a case by case basis.

If you currently have non-U.S. or dual citizens in sensitive positions, a review of those personnel must be made by CNO (N90N2) immediately. If you have a compelling need to hire a foreign national for a position in the furtherance of DON mission and for which a suitable U.S. citizen is not currently available, a U.S. citizenship waiver request package must be completed and submitted to CNO (N90N2). Each package will be reviewed and if there are no issues or questions on the information provided, Personnel Security Branch (attn: Ms. Shirley Maddox-Stubbs) will notify your Command in writing after 10 working days with the determination on interim authority to hire. The expected time for final determination of authority to hire is approximately 4-6 months.

## TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	2
TABLE OF CONTENTS	3
BACKGROUND	4
REQUIREMENT	5
TAKING ACTION	6
APPENDICES	
AP1. Appendix A, CHECKLIST FOR WAIVER OF CITIZENSHIP FOR NATIONAL SECURITY POSITIONS	7
AP2. Appendix B, TEMPLATE LETTER FOR SUBMITTING OFFICIAL U.S. CITIZENSHIP REQUIREMENT WAIVER REQUEST	9
AP3. Appendix C, POSITION-DESIGNATION ACCESS TRACEABILITY MATRIX	12

## BACKGROUND

We all rely daily on access to information to get our job done. From sharing sensitive files with each other on the network to emailing, the ability to create, read, write, and edit files in a shared environment makes it much easier to access needed information. And we all know the importance of allowing clinicians ease of access to protected health information (PHI) in order to provide effective healthcare.

But increased access to data also makes it easier for unauthorized access to sensitive information. Requirements must be in place to grant role-based access to information and information systems. What you may not realize is that the role of a provider is an example of a non-critical sensitive position that requires U.S. citizenship.

The Department of Defense (DoD) and the Department of the Navy (DON) have established requirements to help mitigate the risk of attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.<sup>1</sup> Designation of sensitive and information technology (IT) positions helps distinguish authority and responsibilities for employment related determinations, and provides a fundamental basis for granting authorized access to sensitive information and information systems. This applies to all DON employees and equally to all DON contractors, consultants, and civilian employees.

According to DoD 5200.2-R, Personnel Security Program, U.S. citizenship is a basic condition for access to classified information and assignment to sensitive national security positions. Assignment of personnel to sensitive national security positions requires appropriate background investigations and additional requirements exist for designating foreign nationals to sensitive positions<sup>2</sup>.

Within DON, sensitive duties (with or without IT responsibilities) have been designated as national security positions and as such, require US citizenship. The Office of Personnel Management (OPM) set forth three sensitivity levels and one non-sensitive level for determining national security positions<sup>3</sup>:

1. Special-Sensitive (SS) Potential for inestimable impact and/or damage
2. Critical-Sensitive (CS) Potential for grave to exceptionally grave impact and/or damage
3. Non-critical Sensitive (NCS) Potential for some to serious impact and/or damage
4. Non-Sensitive (NS) Potential for no impact and/or damage as duties have limited relation to the agency mission

Each of these positions are aligned with DON IT positions<sup>4</sup> in SECNAVINST 5510.30 to ensure an appropriate level of background investigation and position suitability. The table below summarizes the U.S. citizenship requirements for sensitive positions.

**Note:** the position descriptions provided below and examples in Appendix C are not definitive and intended only as guidance. Each command must designate position sensitivity commensurate with (1) the following criteria (source: SECNAVINST 5510.30) and, (2) coordinated determination by the Personnel Program Manager, the Position Supervisor (or Program Manager), the Security Manager, and the appropriate IT Authority for IT positions. Position designations will be at the highest level required by the incumbent's specific duties. When the level of potential damage or privilege and other position characteristics appear to indicate differing levels of designation, the higher designation should always be used.

<sup>1</sup> Definition of an security incident from the HIPAA Security Rule.

<sup>2</sup> Not to be confused with access to classified information by non-U.S. citizens. When there are compelling reasons to grant access to classified information to an immigrant alien or a foreign national in furtherance of the mission of the DoD, such individuals may be granted a "Limited Access Authorization" (LAA), which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years. *Source: DoD 5200.2-R.*

<sup>3</sup> 5 CFR, 732.201

<sup>4</sup> Any position in which the incumbent has access to DON IT systems and/or performs IT-related duties with varying degrees of independence, privilege, and/or ability to access and/or impact sensitive data and information. Given the direct supporting relationship of DON IT systems to the DON national security mission, most DON IT positions are sensitive.

Position Sensitivity Designation	IT Desig.	US Cit. Req'd	Waivers Permitted	Description of Position
Critical Sensitive (CS)	IT-I	Yes	For incumbents only – CNO (N09N2) approval required	Personnel responsible for the development and administration of DoD computer security programs
Noncritical-Sensitive (NCS)	IT-II	Yes	Infrequent – CNO (N09N2) approval required	Personnel accessing PHI or Privacy Act Information through DoD Systems
Nonsensitive (NS)	IT-III	No	Not necessary, technical limitations and protections negate the ability to access sensitive information, and render the positions nonsensitive	Personnel working only with Microsoft Office Suite applications on DoD systems such as data management and customer support

## REQUIREMENT

So why is U.S. citizenship a requirement for the role of a provider? From SECNAVINST 5510.30, any position that involves access to information requiring protection under the Privacy Act of 1974 is considered a NCS/IT-II position (see the above table). A patient's medical record contains much of the same information that is protected under the Privacy Act: name, social security number, address. (Recall that U.S. citizenship is a requirement for all IT-II and IT-I positions.) Also, DoD 8500.2 delineates subcategories of sensitive information that include "information the disclosure of which would constitute an unwarranted invasion of personal privacy." HIPAA data is listed as an example of such sensitive information.

In addition, AHLTA<sup>5</sup>, like its predecessor CHCS II, is DoD's electronic health record that permits retrieval of healthcare information by a patient's name or social security number. Whenever a Federal agency or its contractor maintains information about individuals and retrieves it by a personal identifier, that system is a Privacy Act System of Record<sup>6</sup>. In either case, the provider is accessing information that requires protection under the Privacy Act.

The U.S. citizenship requirement applies to **all** personnel in **any** national security / sensitive assignment or duty, designated as IT-I or IT-II sensitivity. A guide for identifying DON positions in terms of sensitivity designation and foreign national access is contained in Appendix C. This is not intended to be exhaustive nor conclusive; each Command must determine appropriate position/sensitivity designations in accordance with DoD and DON requirements.

In those rare instances where a qualified U.S. citizen is not available to occupy a NCS/IT-II or CS/IT-I position, the Command must request a U.S. Citizenship Requirement Waiver Procedures for Persons Nominated to Occupy DON Sensitive and IT Positions. This includes Command medical employees who have been hired as consultants, contractors, and Federal employees with IT system access who are non-U.S. citizens. Requests for waiver of U.S. citizenship requirements for assignment to sensitive positions must be submitted to, and approved by, the Chief of Naval Operations prior to assignment. **Requests must be complete and sent to:**

Chief of Naval Operations (CNO/N09N2)  
 Personnel Security Branch  
[www.navysecurity.navy.mil](http://www.navysecurity.navy.mil)  
 Attn: Ms Shirley Maddox-Stubbs

Waivers for assignment of non-U.S. personnel to national security / sensitive assignments or duties are granted after the required investigation is completed and other pertinent data is assessed. Temporary authority to hire non-U.S. personnel to national security / sensitive assignments or duties pending the results of security investigations may be granted **only by** CNO (N90N2) on a case by case basis. If you currently have non-U.S. or dual citizens in NCS/IT-II or CS/IT-I positions, a review of those personnel must be made by CNO (N90N2) immediately. Corresponding background investigation fees to OPM are paid by DON.

<sup>5</sup> AHLTA gives healthcare providers access to data about beneficiaries' conditions, prescriptions, diagnostic tests and additional information essential to providing quality care. See <http://www.ha.osd.mil/ahлта/> for more information

<sup>6</sup> The Privacy Act 1974 requires a Federal agency to publish in the Federal Register a Notice when it establishes a system of records. The notice must describe the information about individuals the system will contain, and how an individual can obtain any information pertaining to him or her in that system. It ensures those maintaining protected information (PI) are aware of their responsibilities to safeguard and protect personal information.

## U.S. CITIZENSHIP REQUIREMENT WAIVER PROCEDURES FOR PERSONS NOMINATED TO OCCUPY DON SENSITIVE AND INFORMATION TECHNOLOGY (IT) POSITIONS

The requirements described above were reasserted in SECNAVINST 5510.30, "Personnel Security Program", which was released in June 2006. The U.S. citizenship requirement waiver procedures are documented in SECNAVINST 5510.30 Exhibit 5-B. A checklist for waiver of citizenship requirements for national security positions is included in Appendix A. The checklist outlines all necessary provisions that must be met prior to submitting your official request to CNO (N09N2).

### TAKING ACTION

If you have a compelling need to hire a foreign national for a position in the furtherance of DON mission and for which a suitable U.S. citizen is not currently available, a U.S. citizenship waiver request package should be completed following this guidance and submitted by the Command Security Manager with assistance from Human Resources. Each package will be reviewed and if there are no issues or questions on the information provided, Personnel Security Branch (Ms. Shirley Maddox-Stubbs) will notify your Command in writing after 10 working days with the determination on interim authority to hire. The expected time for final determination of authority to hire is approximately 4-6 months.

If you currently have non-U.S. personnel for whom a waiver of U.S. citizenship has not been requested, your Command likely does not have approval for those personnel to work in sensitive positions. Until interim or final authorization is received from the CNO (N90N2) Personnel Security Branch Office, those personnel must be removed from respective duties. The time-line described above for receiving interim and final authority to hire from CNO (N90N2) is identical for existing personnel.

The procedures in the enclosed checklist together with the attached template letter provide the necessary steps for your facility Security Manager to complete and submit official requests. CNO (N09N2) will review and coordinate the request with the appropriate authorities to determine if sufficient justification exists and if adequate security protections are in place. If approved, your Command will be advised and the request for investigation will be forwarded to OPM. Upon completion, investigations conducted on non-U.S. citizens that are to occupy sensitive positions will be forwarded to CNO (N09N2) for the required personnel security determination. Your Command will be advised of the adjudicative results accordingly.

Security Managers should use the checklist in Appendix A to process the waiver request for each individual. The checklist captures all necessary procedures, and provides a convenient tool for ensuring accurate completion of requests. Note, in addition to the items in the checklist, a copy of your Command's Security Instruction must accompany the package as an enclosure. A sample letter for submitting official waiver requests can be found in Appendix B.

Please direct questions to LT Mark Beckner, Navy Medicine Information Assurance Program Manager at (301) 319-1189 or by email: [mabeckner@us.med.navy.mil](mailto:mabeckner@us.med.navy.mil).

**APPENDIX A: CHECKLIST FOR WAIVER OF CITIZENSHIP REQUIREMENTS FOR NATIONAL SECURITY POSITIONS**

Executive Order 11935, and SECNAV M-5510.30 Chapter 5 and exhibit 5B establish requirements for federal employment of Non-U.S. Citizens in sensitive/national security positions. The provisions outlined below must be met prior to submitting your requests CNO (N09N2):

<b>WAIVER REQUESTS OF CITIZENSHIP REQUIREMENTS FOR NATIONAL SECURITY POSITIONS must include the following:</b>	<b>Included or adequately explained</b>	<b>Missing or incomplete</b>	<b>Additional Comments</b>
Request is for a waiver of the US citizenship standard for persons nominated to occupy DON sensitive positions <u>without IT duties</u> .			
A detailed justification for the waiver request including compelling need in the furtherance of the DON mission, <u>signed by commanding officer</u> , to include: full identity of the applicant, applicant's country of origin, and applicant's special expertise. (Compelling reasons may exist in those circumstances where a non-US citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not currently available.)			
The original completed investigation request forms (SF 86, all releases and fingerprint cards).			
Subject has initialed and dated all places on the SF-86 where corrections have been made.			
A copy of the OPM employment approval or other documented authority under which the offer of employment to a non US citizen is permitted. Indicate whether the proposed employee will be hired as excepted service, consultant, temporary employee, seasonal or other.			
Declaration for Federal Employment (Optional Form 306)			
Resume			
Documentation identifying the applicant's immigration status, alien residency and/or other visa status.			
Copy of the position description for which the employed is hired.			
Detailed description of the sensitive duties to be performed or sensitive information to be accessed.			
Detailed description all IT system accesses required.			
Formal command security plan			
Command security plan includes a detailed description of the physical security measures and mechanisms in place to preclude the individual from having access to classified information and/or controlled unclassified information.			

<b>WAIVER REQUESTS OF CITIZENSHIP REQUIREMENTS FOR NATIONAL SECURITY POSITIONS must include the following:</b>	<b>Included or adequately explained</b>	<b>Missing or incomplete</b>	<b>Additional Comments</b>
Command security plan includes description of the information assurance protections implemented, to include the additional administrative, procedural, physical, communications, emanations, computer, information and personnel security measures implemented to minimize the risk (e.g., How the command plans to control and limit the access).			
Detailed security procedures in place to limit access to .mil accounts, and procedures in place on e-mail accounts and signature blocks that identify the individual as a non-U.S. citizen along with his/her country of origin, as required by COMNAVTELCOM.			
Detailed security procedures in place to identify non-U.S. citizens to faculty and students.			
Director, Navy International Programs Office (Navy IPO) foreign disclosure approval of CUI.			
NCIS country-specific counterintelligence briefing addressing the security risks.			

**NOTE**

- Non-US citizen employees who are performing duties under waiver authority are **not** permitted to supervise other employees.
- Supervisors must ensure that safeguards are in place to prevent unauthorized access to FOUO, Privacy Act, and CUI data.
- Access of classified information by the non-US citizen employee is **not** authorized.

## **APPENDIX B: Template Letter for Submitting Official U.S. Citizenship Requirement Waiver Request**

### **Instructions**

1. Please use the checklist in Appendix A in completing this letter.
2. One letter completed for each individual requiring a waiver of U.S. citizenship.
3. Information specific to your command should be entered wherever information is denoted with the placeholders "<>".
4. Command security managers are directed to contact Ms. Maddox-Stubbs or Ms. Stephens if assistance or clarification is required.

Chief of Naval Operations (CNO/N09N2)  
Personnel Security Branch  
[www.navysecurity.navy.mil](http://www.navysecurity.navy.mil)  
Attn: Ms Shirley Maddox-Stubbs, or  
Francine Stephens at [Francine.stephens1@navy.mil](mailto:Francine.stephens1@navy.mil)



**DEPARTMENT OF THE NAVY**

<Name of Activity>  
<Address>  
<City, State Zip-4>

<SSIC>  
<Code/Serial>  
<DD Mon YY>

From: Commanding Officer, <Activity>, <Location>  
To: CHIEF OF NAVAL OPERATIONS (CNO/N09N2)  
PERSONNEL SECURITY BRANCH  
ATTN: MS SHIRLEY MADDOX-STUBBS  
Via: (1) <routing prior to intended recipient, if necessary>  
(2) <next in chain, prior to intended recipient>  
Subj: U.S. CITIZENSHIP REQUIREMENT WAIVER REQUEST FOR <FIRST>  
<NAME> NOMINATED TO OCCUPY DON SENSITIVE POSITION  
Ref: (a) SECNAVINST 5510.30, Department of the Navy  
Personnel Security Program  
(b) Executive Order 11935  
Encl: (1) Original completed SF 86  
(2) Original completed fingerprint cards  
(3) Copy of OPM employment approval or other documented authority  
(4) Immigration status documentation (alien residency,  
And/or visa status)  
(5) Declaration of Federal Employment (Optional Form 306)  
(6) Candidate resume  
(7) Position description for which the candidate is being considered  
(8) Formal Command Security Plan  
(9) Director, Navy International Programs Office (Navy IPO) foreign  
disclosure approval of CUI  
(10) NCIS country-specific counterintelligence briefing addressing the  
security risks

1. This letter serves as official request to waive the U.S. citizenship requirement for <rate> <Last Name>, country of origin <Country of Origin>, per requirements set forth in references (a) and (b). Please find attached the following documentation for CNO (N09N2) review:

a. Original completed investigation request forms, including SF 86 and fingerprint cards;

b. A copy of the OPM employment approval or other documented authority under which the offer of employment to <rate> <Last Name> is permitted;

c. Documentation identifying <rate> <Last Name>'s immigration status, alien residency, and/or other visa status;

d. Declaration of Federal Employment (Optional Form 306);

e. Resume for <rate> <Last Name>;

f. Copy of the position description for which <rate> <Last Name> is being considered;

g. Formal <Activity> Security Plan that includes a detailed description of physical and information assurance security measures and mechanisms;

h. Directory, Navy IPO foreign disclosure approval of CUI;

i. NCIS country-specific counterintelligence briefing addressing the security risks.

2. <detailed justification of compelling reasons requiring assignment, to include special expertise>.

3. <detailed description of the sensitive duties to be performed or sensitive information to be accessed, including all IT system accesses required (e.g., AHLTA)>.

4. <detailed security procedures in place to limit access to .mil accounts, and procedures in place on e-mail accounts and signature blocks that identify the individual as a non-U.S. citizen along with his/her country of origin, as required by COMNAVTELCOM>.

5. <detailed security procedures in place to identify non-U.S. citizens to faculty and students>.

<First-Initial. Last Name>  
Commanding Officer

Copy to:  
NMIMC IA Office  
BUMED IA Office

**APPENDIX C: POSITION-DESIGNATION ACCESS TRACEABILITY MATRIX**

	<b>Position</b>	<b>Desig.</b>	<b>FN</b>	<b>Justification</b>	<b>Reference</b>
<b>Senior Executive Staff</b>	CIO	IT-I	N	Responsibility for development and administration of computer security programs, and also including direction and control of risk analysis and/or threat assessment.	SECNAVINST M-5510.30, 5-3.b.(6)(a)
	CO/XO	IT-I	N	Development or approval of plans, policies, or programs which affect the overall operations of the DON (e.g., policy making or policy determining positions).	SECNAVINST M-5510.30, 5-3.b.(2)
	NCIS	IT-I	N	Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.	SECNAVINST M-5510.30, 5-3.b.(4)
	PAO	IT-I	N	Fiduciary, public contact, or other duties demanding the highest degree of public trust	SECNAVINST M-5510.30, 5-3.b.(5)
	Program Manager	IT-I	N	The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS.	DoD 8510.1-M
	Personnel Program Manager	IT-I	N	Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.	SECNAVINST M-5510.30, 5-3.b.(4)
	Position Supervisor	IT-I	N	Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.	SECNAVINST M-5510.30, 5-3.b.(4)
	Security Manager	IT-I	N	Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.; The security <b>manager must be a U.S. citizen</b> and...	SECNAVINST M-5510.30, 5-3.b.(4), DL1.1.58; 2-3.3.
<b>Provider</b>	Clinical Support	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	Physician, Nurse, etc.	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
<b>Medical Records / Patient Admin</b>	Medical Records	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	PAD	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
<b>Admin Support</b>	Receptionist	IT-II/IT-III	C	<i>designation based on analysis of general position responsibilities.</i>	
	File Clerk	IT-II	C	<i>designation based on analysis of general position responsibilities.</i>	
<b>Facility Support</b>	Facility Support Services	IT-III	Y	Preclude (a) access to system security and network defense systems, or to system resources, (b) visual access to proprietary data, information requiring protection under the Privacy Act of 1974, government-developed privileged information involving the award of contracts, and other protected sensitive information, and (c) ability to input, delete or otherwise manipulate protected sensitive information.	SECNAVINST M-5510.30, 5-3.d.

Y: Waiver of U.S. citizenship **permitted**  
 N: Waiver of U.S. citizenship **not permitted**  
 C: Waiver of U.S. citizenship **conditionally permitted**

	Position	Desig.	FN	Justification	Reference
Business / Finance	Contracting Officer Rep (COR)	IT-II	N	Commands that award <i>classified contracts</i> to industry will appoint, in writing, one or more qualified security specialists as the Contracting Officer's Representative (COR). The COR is responsible to the security manager for coordinating with program managers and technical and procurement officials.	SECNAVINST M-5510.30, 2-7
	Facility Security Officer	IT-II	C	Assignment to duties involving the protection and safeguarding of DON personnel and property	SECNAVINST M-5510.30, 5-3.c.(2)
	Training Head	IT-II	C	Duties involving education and orientation of DoD personnel	SECNAVINST M-5510.30, 2-9.1.-2.
	HIPAA Privacy Officer	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	HIPAA Security Officer	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	Human Resource Personnel	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	Privacy Officer	IT-II	C	Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems...	SECNAVINST M-5510.30, 5-3.c.(8)(b)
	Supervisor of IT-I/IT-II	IT-I	N	Table E3.T1.	DoD 8500.2, Feb 6, 2003
	Special Secret Officer	IT-I	N	Commands in the DON accredited for and authorized to receive, process and store SCI will designate a Special Security Officer (SSO). appointed, in writing, and <b>each will be a U.S. citizen...</b>	SECNAVINST M-5510.30, 2-9.1.-2.
	Top Secret Control Assistant	IT-I	N	A person designated as a Top Secret Control Assistant (TSCA) <b>must be a U.S. citizen and...</b>	SECNAVINST M-5510.30, 2-6.3.
	Top Secret Control Officer	IT-I	N	The TSCO <b>must be a U.S. citizen and...</b>	SECNAVINST M-5510.30, 2-5
Information Technology	Testing Staff	IT-I	N	Table E3.T1.	DoD 8500.2, Feb 6, 03
	PKI Cert Staff	IT-I/IT-II	N	Table E3.T1.	DoD 8500.2, Feb 6, 03
	Security Assistant	?	C	Civilian and military member employees performing admin functions under the direction of the security manager may be assigned in writing without regard to rate or grade as long as they have appropriate clearance. nb: No mention of citizenship requirement.	SECNAVINST M-5510.30, 2-6.2.
	Security Manager Asst.	IT-I	N	Persons designated as assistant security managers must be U.S. citizens,...	SECNAVINST M-5510.30, 2-6.1.
	System Admin	IT-I/IT-II	C	Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and/or management of systems hardware and software. (if under direct technical review of IT-I, then can be designated IT-II)	SECNAVINST M-5510.30, 5-3.b.(6)(f)
	Network Admin	IT-I	N	Responsible for the admin and operation of a network and works with the NSO to ensure the network operates in accordance with Command security policies and procedures. May also be the NSO for his or her particular network.	NAVSO P-5239-08, March 1996
	Administrator (IA privilege)	IT-I	C	Table E3.T1. Examples: Administration of IA devices (e.g., boundary devices, IDS, routers and switches) FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component	DoD 8500.2, Feb 6, 2003
	Administrator (no IA privilege)	IT-II	Y	Table E3.T1.: AIS admin, OS admin, end-user admin, admin of common applications such as email, word processing. (HELPDESK) FN - Under the immediate supervision of a U.S. citizen.	DoD 8500.2, Feb 6, 2003

Y: Waiver of U.S. citizenship **permitted**  
N: Waiver of U.S. citizenship **not permitted**  
C: Waiver of U.S. citizenship **conditionally permitted**

	Position	Desig.	FN	Justification	Reference
Information Management	DAA	IT-I	N	Effective the date of this policy manual, DON non-U.S. citizen employees will <b>NOT</b> be permitted to be assigned or continue assignment to a special-sensitive DAA positions.	SECNAVINST M-5510.30, 5-6.3.a.
	IA PM	IT-I	N	Responsibility for development and admin of computer security programs, and also including direction and control of risk analysis and/or threat assessment.	SECNAVINST M-5510.30, 5-3.b.(6)(a)
	IAM	IT-I	N	(6) Certain IT positions will be designated as CS, and IT-I, due to the potential for grave damage to the national security. CS IT-I positions include those in which the incumbent has: (b) Been designated as IAM or IAO.	SECNAVINST M-5510.30, 5-3.b.(6)(b)
	IAO (w IA admin privileges)	IT-I	N	(6) Certain IT positions will be designated as CS, and IT-I, due to the potential for grave damage to the national security. CS IT-I positions include those in which the incumbent has: (b) Been designated as IAM or IAO.	SECNAVINST M-5510.30, 5-3.b.(6)(b)
	IAO (w/o IA admin privileges)	IT-II	C	<b>FN</b> - With DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the <b>immediate supervision of a U.S. citizen IAM, and have no supervisory duties.</b>	DoD 8500.2, Feb 6, 2003
	Incident Response Mgr	IT-II	N	?? Supervisory duties?? (see ISSO)	
	ISSM	IT-I	N	<u>5239-19</u> : responsible for coordinating computer security efforts within an organization... advise the CO in the event of a serious security incident, and coordinate the response with security personnel. <u>8500.2</u> : E2.1.27. IAM. The individual responsible for the IA program of a DoD information system or organization... may be used interchangeably with ISSM.	NAVSO P-5239-19, August 1996; DoD 8500.2, Feb 6, 2003
	ISSO	IT-I/IT-II	C	<u>5239-19</u> : responsible for operational security within a subset of machines assigned to a particular site or facility. Each organization has at least one ISSO. ...first level of interaction for users experiencing <b>security incidents.</b> <u>8500.2</u> : E2.1.28. IAO. An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization... may be used interchangeably with ISSO, Information Systems Security Custodian, NSO, or Terminal Area Security Officer.	NAVSO P-5239-19, August 1996; DoD 8500.2, Feb 6, 2003
	IT Authority (for IT Positions)	IT-I	N	Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.; and have <b>no supervisory duties.</b>	SECNAVINST M-5510.30, 5-3.b.(4); DoD 8500.2, Feb 6, 2003
	Network Security Officer	IT-I	N	<u>6510.01</u> : IAO. An individual responsible to the IA manager for ensuring the appropriate operational IA posture is maintained for a DoD information system or organization. <u>8500.2</u> : E2.1.28. IAO ... may be used interchangeably with ISSO, Information Systems Security Custodian, <b>Network Security Officer.</b>	CJCSM 6510.01, 25 Mar 2003, Part II -- Definitions; DoD 8500.2, Feb 6, 2003
	Maintenance of IA products	IT-I	C	<b>FN</b> - Under the <b>immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component All</b> - Also subject to IA controls (e.g., PEPF and ECRB)	DoD 8500.2, Feb 6, 2003
	Maintenance of IA-enabled products	IT-II	C	<b>FN</b> - Under the <b>immediate supervision of a U.S. citizen.</b> All - Also subject to IA Controls (e.g., PEPF and ECRB)	DoD 8500.2, Feb 6, 2003

Y: Waiver of U.S. citizenship **permitted**  
N: Waiver of U.S. citizenship **not permitted**  
C: Waiver of U.S. citizenship **conditionally permitted**