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

CNATRAINST 5239.4
N6
7 May 18

CNATRA INSTRUCTION 5239.4

Subj: CYBERSPACE INFORMATION TECHNOLOGY/CYBERSECURITY WORKFORCE QUALIFICATION PROGRAM

Ref: (a) DOD 8140.01
(b) DOD 8570.01-M
(c) OPNAVINST 5239.1C
(d) SECNAVINST 1543.2
(e) SECNAVINST 5239.3C
(f) SECNAVINST 5239.20A
(g) SECNAV M-5239.1
(h) SECNAV M-5239.2
(i) SECNAV M-5510.36

Encl: (1) Definitions
(2) Cyber IT/CSWF Category Model and CNATRA Assigned Specialty Codes
(3) Individual Development Plan
(4) Web Links to References

1. Purpose

a. Provide Chief of Naval Air Training (CNATRA) headquarters and subordinate commands the regulations and guidance governing the Department of the Navy (DON) Cyberspace Information Technology/Cybersecurity Workforce Qualification Program (Cyber IT/CSWFQP). References (a) and (b) establish policy and guidance for the training, certification and management of CSWF across the Department of the Defense (DOD). References (c) through (i) provide direction and guidance for DON Cyber IT/CSWF Management.

b. Establish the Cyber IT/CSWFQP under the direction of references (e) and (h) and in compliance with references (a) through (i).

c. Ensure there is a common set of capabilities among the Cyber IT/CSWF personnel that promotes interoperability, facilitates professional development and training, and develops a workforce of qualified and competent Cyber IT/CSWF professionals.

d. Provides the vehicle for professional improvement, supporting career development and specialized assignments.

e. Provides a means to validate that all Cyber IT/CSWF members have the knowledge and skills deemed necessary to perform their specific job functions, protecting the DOD, DON and Naval Air Training Command (NATRACOM) Cybersecurity (CS) environments.

f. Ensure CNATRA has a competent Information Systems (IS) professional workforce which is appropriately trained and commercially certified in technical and non-technical CS functional areas.

2. Cancellation. CNATRAINST 5239.2A.

3. Definitions. Enclosure (1) of this instruction defines relevant terms.

4. Applicability

a. This instruction applies to all CNATRA military, civilian and contract personnel, who work to design, develop, operate, maintain and defend data, networks, network centric capabilities, computing capabilities and communications across secure classified collateral or unclassified information systems and networks. It also includes personnel that manage risks and protect DON and NATRACOM systems and information.

b. This program is mandatory for all personnel who will be, or are performing Cyber IT/CSWF functions as a primary, part-time, or collateral job to include military, civilian or contract personnel who have privileged access to government information systems or have significant administrative IT responsibilities without regard to rank/grade, rating/designator/Military Occupational Specialty (MOS) Code, occupational series, or job title.

5. Background

a. To standardize and improve the knowledge and skills of Cyber IT/CSWF professionals across the DOD, the Military Services were mandated to implement the Cyber IT/CSWFQP in accordance with references (a) and (b). The Cyber IT/CSWFQP requires the Military Services to identify military and civilian billets with significant IT security responsibilities, identify personnel filling these positions, and ensure they receive specialized training and are commercially certified to perform assigned Cyber IT/CSWF job functions. Policy and implementation guidance for the DON Cyber IT/CSWFQP is promulgated in references (c) through (i).

b. The Cyber IT/CSWF focuses on the operation and management of Cyber IT/CS capabilities for DOD Information Systems (IS) and networks. The Cyber IT/CSWF ensures that adequate security measures and established CS policies and procedures are applied to all IS and networks. The Cyber IT/CSWFQP establishes a baseline of validated education, knowledge and skills that are relevant, recognized and accepted across the DOD.

6. Responsibilities

a. CNATRA Chief of Staff (COS) shall:

(1) Designate a Cyber IT/CSWF-Project Manager (PM). The Cyber IT/CSWF-PM will be responsible for the administration of the Cyber IT/CSWF Program.

(2) Ensure Cyber IT/CSWF-PMs are assigned as a primary duty whenever possible. It is not required to be a new and separate billet; however the position should be filled by a person in a position within the command’s Cyber IT/CSWF.

(3) Promote the professional development and qualification of employees who carry out Cyber IT and CS responsibilities.

(4) Ensure the command has a Cyber IT/CSWFQP that ensures training managers work with Cyber IT/CSWF PM to meet shared Cyber IT/CSWF tracking, training, qualifications and reporting responsibilities;

(5) Authorize the Command Information Systems Security Manager (ISSM) to oversee the Cyber IT/CSWFQP.

(6) Empower the Command Cyber IT/CSWF-PM to ensure compliance.

(7) Assign personnel and training responsibilities to local human resources, administrative and training officers to carry out Cyber IT/CSWF management.

(8) Ensure Cyber IT and CS contractor personnel have the appropriate appointment letter, CS qualification and background investigation. Contracting Officer's Technical Representative must ensure the Command Contracting Officer is aware of contractor personnel not meeting appointment, qualification, or investigation requirements. The Command Contracting Officer will ensure current and future contract Statement of Work (SOW) or Performance Work Statement (PWS) have sufficient language that requires contractor personnel to meet appointment, qualification, and investigation requirements.

b. Cyber IT/CSWF Program Manager (PM) shall:

(1) Be responsible for the administration of the organization's Cyber IT/CSWF Qualification Program. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization or by the command ISSM.

(2) Accountable for reporting, database management, and overall effectiveness of the program and commands and/or subordinate units.

(3) Work with the immediate superior in the chain of command to meet shared Cyber IT/CSWF management oversight and compliance responsibilities.

(4) Ensure Military Service electronic reporting mechanisms are used to allow for consistent data reporting.

(5) Whenever possible, the Cyber IT/CSWF-PM role shall be a primary duty. It is not required to be a new and separate billet or position, but shall be assigned to a person in a position within the command's Cyber IT/CSWF.

(6) Document and maintain the certification status of CSWF personnel. Ensure all required information is properly reflected in the CSWF database(s).

(7) Track and Report on command CS training (including awareness) and certification programs to Administrative Immediate Superior in Command (ISIC) as required.

(8) In the event a Cyber IT/CSWF member fails to achieve qualification compliance, notify the Cyber IT/CSWF member of their status and any required remediation. The command shall put the member in a waiver status (not to exceed six months); pending review of competencies and potential movement to a non-Cyber IT/CSWF position. If a non-Cyber IT/CSWF position is not available, the employee will be subject to other actions, up to and including removal.

(9) Inform the Office of Primary Responsibility (OPR) Cyber IT/CSWF-PM of personnel who are not in compliance and their status.

(10) Be a United States (U.S.) citizen. Non U.S. citizens and contractors may not serve as Cyber IT/CSWF-PM.

c. CNATRA Information System Security Officer (ISSM) shall:

(1) Be responsible for Cyber IT and CS training and qualification compliance;

(2) Ensure all IS users (including contractors) are appropriately trained in accordance with references (e) and (f).

(3) Stabilize workforce rotation in the workplace so training Cyber IT and CS personnel are assigned to Cyber IT and CS jobs commensurate with their qualifications.

(4) Review the Cyber IT and CS structure of the command and identify appropriate staffing requirements.

(5) Ensure Cyber IT/CSWF Individual Development Plans (IDPs) are created that detail specific CS training and qualifications required for compliancy.

(6) Process and submit CSWF certification exam voucher requests to U.S. Navy (USN), Credentials Program Office for approval.

d. Command Information System Security Officer (ISSO) shall:

(1) Assist the ISSM’s in meeting their duties and responsibilities.

(2) Coordinate with the Command Security Manager to ensure that all users have the requisite security clearances and access authorization, and are aware of the CS responsibilities for DOD IS and PIT systems under their purview before being granted access to those systems.

(3) Fulfill both the ISSM and the ISSO roles when circumstances warrant.

(4) Be a U.S. citizen. Non U.S. citizens and contractors may not serve as ISSO.

e. Privileged Users shall:

(1) Be trained, qualified, and designated on the System Authorization Access Request (SAAR) as a Privileged User and through completion of a privileged access agreement (PAA) signed by the ISSM and validated by the Cyber IT/CSWF-PM.

(2) Be appropriately cleared to DON guidance.

(3) Configure and operate IT within the authorities vested in them according to DON CS policies and procedures.

(4) Notify the responsible ISSM, and when appropriate, the Command Security Manager, of any changes that might affect security posture.

(5) Maintain Cyber IT/CSWF qualifications as delineated in appendix 4 of reference (c) as well as maintain the required security clearance.

(6) Understand individual qualification requirements of position assigned and comply with the Cyber IT/CSWF requirements directed in references (a) through (i) by ensuring awareness of being personally accountable and responsible for individual development, training, and qualification compliance requirements.

(7) Routinely check with their local command Cyber IT/CSWF-PM to verify his/her entry within the DON/USN/U.S. Marine Corps (USMC) authoritative manpower, personnel, and readiness databases accurately depicts his/her qualification status.

(8) Be ultimately responsible for the attainment, upkeep, and maintenance of their Cyber IT/CSWF status, to include continuous learning(CL), qualification maintenance, and awareness of Cyber IT/CSWF policies and standards.

(9) Review command PAA annually for completeness and accuracy.

f. Authorized users shall:

(1) Understand and comply with command CS policies and procedures.

(2) Have a current SAAR-N signed and on file with the Command ISSM.

(3) Complete and report minimum CS awareness and training compliance.

(4) Immediately report all CS-related events (e.g., data spill) and potential threats and vulnerabilities (e.g., insider threat) to the appropriate ISSO or, in the absence of an ISSO, the ISSM and the Command Security Manager.

(5) Protect authenticators commensurate with the classification of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate ISSO and the Command Security Manager.

(6) Protect terminals, workstations, other input or output devices and resident data from unauthorized access.

(7) Inform the responsible ISSO when access to a particular DOD IS or PIT system is no longer required (e.g., completion of project, transfer, retirement, resignation).

(8) Use DOD IT only for official and authorized purposes.

(9) Prevent relocation of or change to DOD IT equipment or the network connectivity of equipment without proper authorization.

(10) Prevent the introduction or use of software, firmware, or hardware that has not been approved by the Authorizing Official (AO) or a designated representative of DOD IT.

7. Cyber IT/CSWF Qualification Program Guidance.

a. The Cyber IT/CSWFQP validates a Cyber IT/CS practitioner's knowledge and understanding of facts, concepts, and principles that the DOD Cyber IT/CS community deems critical to successfully perform functions, implement programs, and pursue missions necessary to deliver cyber capabilities to the DON. The community includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risks and protect DON systems and information.

b. The Cyber IT/CSWFQP is mandatory for all Cyber IT/CS personnel who will be or are already performing Cyber IT/CS functions as a primary and/or additional duty on behalf of (and as specified by) CNATRA or are working towards qualification for assignment to a CS position. This initiative is intended to ensure that there is a common set of capabilities among Cyber IT/CS personnel that promotes interoperability, facilitates professional development and training, and develops a workforce of qualified Cyber IT/CS professionals.

c. As a condition of privileged access to any information system, personnel performing Cyber IT/CS tasks described in reference (h) must satisfy both preparatory (initial training) and sustaining DOD Cyber IT/CS qualifications requirements. Additionally, personnel assigned to CNATRA and its subordinate commands Cyber IT/CS positions requiring privileged access must complete a PAA.

d. The qualification requirements of this manual apply to DOD civilian employees, military personnel, local nationals, and support contractors performing the Cyber IT/CS roles.

e. The CNATRA Cyber IT/CSWFQP is intended to produce Cyber IT/CS personnel with a baseline understanding of the fundamental Cyber IT/CS principles and practices related to their assigned position. Each category, specialty area, and proficiency level has specific qualification requirements. Meeting these requirements will require a combination of credentialing (education, formal training and certification), continuing education (CE), and experience activities (on-the-job training), performance qualification standards (PQS), or job qualification requirements (JQR). The initial activities (training, testing, on the job training and practice) required for qualification requirements will be provided by the DON at no cost to government employees (military or civilian). If, at any time, the employee allows the certification to expire, it will be the employee’s responsibility to pay for the new certification.

f. Only approved training, education and certifications, and job qualification requirements documented in matrices listed in appendix 4 of reference (h) will be used to satisfy CSWFQP requirements. The matrices outline minimum requirements.

g. Approved training, education and certifications will demonstrate close correlation to the Cyber IT/CS categories, specialty areas, and proficiency levels and demonstrate portability throughout the DOD, the Federal Government, and the private sector.

h. Individuals assigned to CNATRA and its subordinate commands not meeting qualification requirements of their Cyber IT/CS position must be reassigned to other duties, consistent with applicable law. Until qualifications are attained, individuals in Cyber IT/CS positions not meeting qualification requirements may perform those duties under the direct supervision of an appropriately qualified individual. If the individual fails to achieve qualification within six months of signed Cyber IT/CSWF letter of designation, they must be removed from the Cyber IT/CS position.

i. Personnel utilizing Cyber IT/CS certification to meet Cyber IT/CS training/education requirements must adhere to all recertification policies set by their certification provider and ensure that their certifications stay active. This means that the certification holder must maintain the certification vice taking the exam each time the certification expires.

j. To support Cyber IT/CS professionals the DoD Information Assurance Support Environment (IASE) provides DOD CS and CS policy, training requirements, and DOD-sponsored training. The IASE is located at http://iase.disa.mil/.

k. Contractor personnel supporting Cyber IT/CS roles shall obtain the appropriate DOD-approved baseline qualification standards prior to specialty-related task(s). They may be provided an appropriate amount of time to complete DON position specific qualification including PQS/JQR if required. The contracting officer will ensure that contractor personnel are appropriately qualified. Additional training on local or system procedures may be provided by the DOD organization receiving services. The DOD may be required to provide qualification training to contractors when it is not reasonably available in the commercial sector or for DOD unique technology or processes.

8. Cyber IT/CSWF Personnel Management

a. Personnel management includes identifying Cyber IT/CSWF personnel, documenting their information and maintaining their information. Personnel information exists in various Navy and Marine Corps military personnel and training systems and in the Defense Civilian Personnel Data System (DCPDS). Not all required personnel data resides in these systems, nor is it readily available to the Cyber IT/CSWF-PM from those databases. The Navy authoritative manpower, personnel and readiness databases will capture and maintain military and civilian CS personnel information.

b. Identifying Cyber IT/CSWF Personnel

(1) Uniformed Cyber IT/CSWF personnel remain a part of the Cyber IT/CSWF regardless of whether currently assigned to a Cyber IT/CSWF position.

(2) Civilian personnel are considered as part of the Cyber IT/CSWF when assigned to a Cyber IT/CSWF position.

(3) Cyber IT/CSWF personnel may be identified in the following ways:

(a) DON Cyber IT/CSWF code and/or DOD Function are a part of the personnel record in a military personnel system or in DCPDS.

(b) Identified military code such as Military Occupation Specialty (MOS), Navy Enlisted Code (NEC), Sub Specialty Code (SSC) or Additional Qualification Designator (AQD) is a part of the personnel record.

(c) Listed as a member of the Cyber IT/CSWF with the appropriate DON Cyber IT/CSWF code in the Navy authoritative personnel and readiness databases.

c. Documenting Cyber IT/CSWF Personnel Information

(1) Cyber IT/CSWF personnel information includes the designation as a member of the Cyber IT/CSWF as well as information related to training, education, credentialing, individual qualification, continuing education, and CS team assignment information.

(2) If USN Authoritative Data Sources do not include required Cyber IT/CSWF manpower data elements, the DON Cyber IT/CSWF enterprise tracking tool (TWMS) will be used to record and maintain the information.

(3) Contractor records will be recorded in the personnel section of the TWMS Cyber IT/CSWF module. They will be imported from Defense Enrollment Eligibility Reporting System (DEERS) for those with a Common Access Card (CAC) or entered locally as a new record if no CAC is assigned.

d. Maintaining and Modifying Cyber IT/CSWF Personnel Information

(1) The CNATRA Cyber IT/CSWF-PM is responsible for the maintenance of Cyber IT/CSWF personnel information. The Cyber IT/CSWF-PM shall ensure the record is maintained within the Navy authoritative manpower, personnel and readiness databases while personnel are assigned, a copy is included in transfer packages for personnel and follow-on organizations use, and that personnel have access to their information.

(2) Maintenance of Cyber IT/CSWF personnel information required by military personnel and training systems is maintained in those systems. For civilians, if the information is required by DCPDS it shall be maintained there. Policy regarding updating of military and civilian systems must be followed to update these systems. Navy authoritative personnel and readiness databases will access this information and aggregate for the individual's, Cyber IT/CSWF-PM and DON, USN, USMC Cyber IT/CSWF leadership use.

(3) Information residing only in Navy authoritative manpower, personnel and readiness databases will be the responsibility of the individual and the Cyber IT/CSWF-PM. Changes will be made in accordance with Navy authoritative personnel and readiness databases procedures available within the database program.

(4) Cyber IT/CSWF-PMs shall review workforce information in Navy authoritative personnel and readiness databases at least semi-annually and ensure that it remains current and accurate.

(5) Cyber IT/CSWF-PMs will ensure that Cyber IT/CSWF personnel data is captured in the DON Cyber IT/CSWF enterprise tracking tool (TWMS). In those cases where the information is not available from the personnel or training automated database system, then the Cyber IT/CSWF-PM will enter directly into the DON Cyber IT/CSWF enterprise tracking tool (TWMS).

(6) CNATRA's Cyber IT/CSWF-PMs will report Cyber IT/CSWF metrics to Commander, Naval Air Force, US Pacific Fleet (COMNAVAIRPAC) ISSM annually to meet Federal Information Security Management Act (FISMA) reporting compliance.

9. Cyber IT/CSWF Learning Continuum

a. Cyber IT/CSWF education, training and certification are key components in the overall qualification of the workforce. Continuous learning is the component of workforce qualification that addresses the requirements necessary to keep the workforce current. Education, training, certification, and continuous learning will all be mapped to specialty areas within the framework and will be based upon the mapping of Specialty Area tasks and proficiency levels. When appropriate, associated KSAs may be used in the mapping process. Security and OS/CE education, training, and certification will be required of workforce personnel. For the CNATRA Cyber IT/CSWF Qualification Program, academic degrees, military course completion credentials and/or Cyber IT/CSWF certifications may be used to meet the knowledge requirements piece of qualification.

b. The Cyber IT/CSWF learning continuum is geared toward continuous improvement throughout an individual’s career. It includes both wide ranging CS and IT learning and Navy unique training. The continuum is depicted in the requirements outlined in the appendix 4 of reference (h).

c. Elements of the individual learning continuum include:

(1) Military Training

(2) Certification

(3) Academic Degree Programs

(4) Continuous Learning

(5) On the Job Experience (PQS/JQR)

(6) Individual Development Programs

d. The CNATRA Cyber IT/CSWF Qualification Program will center upon credentialing, where credentials can be earned through formal certifications, educational degrees or completion of formal military training. Other learning opportunities included in continuous learning will be utilized to maintain credential currency. New IT training provided in conjunction with system installation, if not a part of a formal military or recognized certification program, will be considered as interim until such time as it becomes part of a formal program. All approved education, training, and certification programs will be included in the Cyber IT/CSWF Qualification Matrix (appendix 4 of reference (h)). Continuous learning opportunities will be approved in accordance with certification provider standards, academic degree requirements and military training guidelines.

10. Cyber IT/CSWF Education

a. Cyber IT/CSWF education is collegiate-level education obtained through programs leading to an academic degree and that continuing education required to keep a degree current.

b. Cyber IT/CSWF education may be obtained through completion of approved and relevant, CS degree programs (associate, bachelor, or advanced degree.)

c. Education must be accurately reported into the Defense Civilian Personnel Data System (DCPDS) with all transcripts uploaded by the individual employee into the current Navy authoritative personnel and readiness database (TWMS). As noted when employees enter this information and affix their digital signature in DCPDS, falsified data in DCPDS could result in fines more than $10,000 or imprisonment of not more than 5 years, or both.

d. Cyber IT/CSWF education may also be obtained through completion of approved Federal and Military Service Degree programs.

e. Approved educational programs will be identified in the Cyber IT/CSWF Qualification Matrix mapped to specialty areas and proficiency levels.

11. CYBER IT/CSWF TRAINING

a. Training requirements are aligned to the DON Cyber IT/CSWF structure and career progression. The continuum will include provisions for Cyber IT/CSWF personnel to gain and maintain proficiency in necessary skills to perform Cyber IT/CSWF tasks. Approved training may be attained through:

(1) Formal military training/course

(2) Formal industry training

(3) Cyber IT/CSWF exercises

b. Approved training programs will be identified in the Cyber IT/CSWF Qualification Matrix mapped to specialty areas and proficiency levels.

12. Cyber IT/CSWF Certification

a. Certifications are typically earned from a professional society and must be renewed periodically, or may be valid for a specific period of time. Certifications are one way for organizations to credential individuals with specific skill sets; they are portable, and do not rely on one company's definition of a certain job. They can enable workforce members to stand out as having necessary professional skills and provide an impartial, third-party endorsement of an individual's professional knowledge and experience.

b. The certifications list contained within the National Initiative for CS Careers and Studies (NICCS) portal supports the DON Cyber IT/CSWF framework. These certifications are mapped to the DON Cyber IT/CSWF framework by specialty area and proficiency level.

c. Certification will be standardized across the DON to provide the necessary consistency among military, civilian, and contractor job roles and responsibilities to ensure interoperability of all segments of the Cyber IT/CSWF.

d. Cyber IT/CSWF personnel with privileged access (military, civilian, or contractor) who use certification as a means to fulfill the “Minimum Credential” criteria within the Cyber IT/CSWF Qualification Matrix must hold a current and maintained version of the certification tied to their assigned specialty area.

e. Cyber IT/CSWF personnel with privileged access (military, civilian, or contractor) who use certification as a means to fulfill the “Minimum Credential” criteria within the Qualification Matrix, and whose certification expire, will have their privileged access revoked and may not continue assigned duties within the specialty area.

f. The Cyber IT/CSWF member must ensure all maintenance fees are applied in accordance with the certification agency’s maintenance fee requirements.

g. The Cyber IT/CSWF member must hold and maintain their certification in accordance with the certification agency’s CL requirements.

h. The Navy’s Credentials Program Office/Navy Credentialing Opportunities On-Line (COOL) may fund eligible Navy military and DON civilian Cyber IT/CSWF personnel’s initial certification exam and annual maintenance fees based on the users specialty area codes and experience levels. Additional information can be found on their website at https://www.cool.navy.mil.

(1) Navy COOL can fund the initial certification to meet Cyber IT/CSWF specialty area certification requirement and annual maintenance fees, but only for the year it is due (not in advance; not in arrears).

(2) Navy COOL will not fund for study/prep materials, memberships, continuous learning or other non-certification fees.

i. Cyber IT/CSWF personnel obtaining commercial certification(s) for the purpose of Cyber IT/CSWF qualification shall have their certification recorded in TWMS. Identification of certification specifics within TWMS will be one of the criteria required before DON payment of expenses including certification provider continuing education and/or certification maintenance fees.

j. Certified Cyber IT/CSWF should routinely check with their local command Cyber IT/CSWF-PM to verify their entry within the Navy authoritative manpower, personnel and readiness databases accurately depicts their qualification status.

k. The CNATRA Cyber IT/CSWF-PM has the requirement to ensure their Cyber IT/CSWF personnel are qualified. However, ultimately, it is the individual Cyber IT/CSWF member’s responsibility to comply with Cyber IT/CSWF qualification requirements and earn and maintain their own certification. The individual Cyber IT/CSWF member must be proactive and keep appraised of changes/updates that the certification agency makes to their certification requirements. Cyber IT/CSWF personnel should not rely on the certification agency to inform them of changes.

l. In the event the Cyber IT/CSWF member fails to achieve qualification compliance, the Commander/Commanding Officer shall notify the Cyber IT/CSWF member of their status and any required remediation. The command shall put the member in a non-Cyber IT/CSWF position, pending review of competencies and potential to achieve qualification. If a Cyber IT/CSWF position is not available or the command determines that the person will not be able to achieve qualification, then the employee will be subject to other action, up to and including removal.

13. Cyber IT/CSWF Continuous Learning Program

a. The DON Cyber IT/CS continuous learning program (CLP) is structured to support the continuing professional development of the CSWF member throughout their career. The CLP will include education, training, certification and other activities that support the sustainment and continued improvement of the capabilities of the DON Cyber IT/CSWF.

b. The overarching goal of the CLP is to improve cyber IT and CS operations, mission effectiveness and increase readiness across the cyber domain. This program provides the vehicle for personal improvement supporting career development and specialized assignments. Depending on the nature of the organization’s work, workforce responsibilities, and the stage of organizational and personal development, training needs will vary. Ideally government personnel will approach CL with focused and targeted training and education and or technical knowledge and skills commensurate with the individual’s rank/grade.

c. Professional or career development and CL should be accomplished through a blended solution of formal classroom training, experience, and electronic media. Learning activities may range from on the job training to operational exercises to accredited education in accordance with reference (e). All training completed for CL credit must be provided to the Cyber IT/CSWF-PM to ensure that it is recorded correctly within the Navy’s reporting system.

d. All CNATRA civilian, military, and contract support Cyber IT/CSWF personnel will participate in the CLP commensurate with their occupation, rank/grade, and position. CLP requirements are as follows:

(1) Per reference (d), Cyber IT/CSWF members shall complete 40 hours of CL activities annually; however, if circumstances preclude 40 hours in a single year, an individual may participate in 80 hours within a two year period to satisfy the requirement. Additionally, hours completed in a previous year may be used to meet the following year’s requirement if approved by the first line supervisor. Hours may not be carried over further than the next consecutive year.

(2) General Cyber IT/CSWF CLP activities may include, but are not limited to, training in multiple CS specialties, leadership training, program management, joint warfighting tactics, ethics, acquisition, and rotational and developmental assignments. The DON Cyber IT/CSWF CL steering group will identify and approve general Cyber IT/CSWF CLP materials and sources. Additionally, commands may identify and submit CL activities through their chain of command to the steering group for review and approval.

(3) All CL required for maintaining currency of commercial certification will be defined by the certification provider. CL credits obtained in support of commercial certification maintenance or sustainment can be used to meet overall DON Cyber IT/CSWF continuous education requirements. Note: If the commercial certification requires less than 40 hours per year, the member must also obtain the difference in hours between the vendor certification requirement and the overall 40 hour DON CLP requirement by completing additional general Cyber IT/CSWF continuous learning activities. It will be the responsibility of the certification holder to verify the Navy’s CLP activities they wish to apply towards their associated certification meet the certification agency’s CL requirements.

(4) The annual CL period start date is the beginning of the calendar year. If the CL requirement is part of a commercial Cyber IT/CSWF certification, the start date is the date identified by the certification vendor.

14. Cyber IT/CSWF Qualifications

a. The Cyber IT/CSWF Qualification Program includes all elements required for a person to qualify to carry out CS work. This includes security and operating system knowledge skills, abilities and proficiencies. The program relies on assessment of a person’s ability to carry out the individual and team responsibilities of the Cyber IT/CSWF position within the command’s organization. Military training programs, academic education, commercial training and certification programs, laboratory and exercise simulation environments and on the job training and practical ability demonstration all play a part in the program. Additionally, the program includes proficiency level qualification requirements so that the individual is qualified based on their ability and the requirements of the position. Proficiency levels also provide a guide to the individual and the supervisor supporting the continuous learning element of the program.

b. The Cyber IT/CSWF structure differs significantly from the previous Information Assurance workforce structure, it is now based upon the actual specialties and proficiency needed for the specific work/billet, not the general area and system/network size. The structure also provides the means to move to a more focused qualification regimen. By utilizing specialty areas and proficiency levels, the DON will identify appropriate training, education and certification requirements along with individual proficiency demonstration in the laboratory and on the job. This process culminates in the qualification of personnel through OJT, PQS or JQR procedure.

c. Cyber IT/CSWF Workforce Proficiency Levels. These levels are based on the employees experience and possible paygrades.

(1) Entry/Apprentice – Basic understanding of computer systems and related CS software and hardware components.

(a) 1-3 years’ experience (recommended)

(b) Enlisted E-1 through E-4

(c) Officer O-1 through O-2

(d) Civilian Grades 5, 7 and 9

(2) Intermediate/Journeyman – Working knowledge and application of information systems security operational characteristics for a variety of computer platforms, networks, software applications, and operating systems.

(a) 4-6 years' experience (recommended)

(b) Enlisted E-5 through E-6

(c) Officer O-3 through O-4

(d) Civilian Grades 9, 11, 12

(3) Expert/Master – Advanced application and mastery of information systems, plans, and functions, and is responsible for the management of complex projects and initiatives with large scope.

(a) 7+ years' experience (recommended)

(b) Enlisted E-7 through E-9

(c) Officer O-5 through O-6 / W-2 through W-5

(d) Civilian grades 13 and above

d. Cyber IT/CSWF Qualification Requirements.

(1) All CNATRA Cyber IT/CSWF personnel (active duty, civilian, and contractors) are directed to obtain and maintain qualification or risk removal from the Cyber IT/CSWF position. This applies to all CNATRA Cyber IT/CSWF personnel, regardless of military specialty, civilian job series, or contract. Cyber IT/CSWF personnel who fail to maintain qualification are a weakness in their local command's (and network) security posture. Commanding Officers shall assign unqualified military and civilian personnel to a supervised status for qualification/requalification or remove unqualified personnel from their Cyber IT/CSWF position while requalification is completed. Those who fail to requalify shall be permanently removed from the Cyber IT/CSWF.

(2) Military and government personnel filling Cyber IT/CSWF positions shall obtain the appropriate DON-approved baseline job qualification standards within six months of assignment. The commanding officer will ensure that military and civilian personnel are appropriately qualified.

(3) Contractor personnel supporting CS shall obtain the appropriate DON-approved baseline job qualification standards prior to being engaged. Contractors have up to six months to obtain the DON Specialty Area Qualifications outlined in (appendix 4 of reference (h)). The Contracting Officer will ensure that contracts requiring Cyber IT/CSWF personnel contain the required CS language and that the contracting organization ensures personnel meet qualification requirements. Additional training on local or system procedures may be provided by the DOD organization receiving services. The DON may be required to provide qualification training to contractors when it is not reasonably available in the commercial sector or for the DON unique technology or processes.

(4) Cyber IT/CSWF PQS/JQR are applicable to all personnel conducting Cyber IT/CS functions, including DOD Information Networks (DoDIN) Operations, Defensive Cyberspace Operations (DCO), system development and acquisition, risk management, and vulnerability assessments supporting the DoDIN. This applies to military, government civilian and contract support personnel.

(a) The PQS/JQR is a compilation of the minimum knowledge and skills that an individual must demonstrate in order to qualify to stand watches or perform other specific CS tasks. The objective of Cyber IT/CSWF PQS/JQR program is to standardize and facilitate these qualifications.

(b) The DON will develop PQS/JQR procedures to include fundamentals, system and positions/watch station requirements. The qualification procedures will address CS and operating system/computing environment/tool requirements. Although not part of initial qualifications, continuing education is the key element in maintaining qualification currency.

(c) CNATRA N6 shall tailor qualification packages by reviewing the Service Level Qualification package by one or more qualified individuals. The department will delete any portions covering systems and equipment not installed in their organization. The department will add any line items, fundamentals, systems and watch stations/workstations that are unique to the command but not already covered in the package. Finally the package will be reviewed by the cognizant director/department head and required changes approved by the COS/Chief Information Officer (CIO) or designated representative. CNATRA N6 will retain the approved master copy on file for use in tailoring individual packages.

(d) The Cyber IT/CSWF PQS/JQR is divided into three sections. The 100 section (fundamentals) contains the fundamental knowledge from technical manuals and other text necessary to satisfactorily understand the CS and OS/CE concepts and processes. The 200 section (systems) is designed to provide basic information on the Operating System (OS)/CE/Tools that will be required to be used at an organization to carry out the tasks associated with a position/watch station. The 300 section (Watch Stations) lists the tasks required to be satisfactorily performed in order to achieve final PQS/JQR completion for a particular position/watch station.

15. Enforcement

Personnel assigned to Cyber IT/CSWF billets who fail to achieve qualification within six months of assignment MUST be removed from the Cyber IT/CSWF position.

a. Commanding Officers shall assign unqualified military and civilian personnel to a supervised status for qualification/requalification or remove unqualified personnel from their Cyber IT/CSWF position while requalification is completed.

b. Contract personnel failing to obtain or maintain the required Cyber IT/CSWF position qualifications shall be removed from contract service.

c. Personnel who fail to requalify shall be permanently removed from Cyber IT/CSWF.

16. Deliverables/Reports. All required reports will be generated in accordance with the current Secretary of the Navy (SECNAV) and DOD policies and maintained by Cyber IT/CSWF-PM.

17. Information Collection Requirements. The Cyber IT/CSWF-PM may be required to collect specific information regarding all Cyber IT/CSWF members and report to higher echelon commands as directed.

18. Updates. CNATRA N6 is responsible for required reviews and update of this instruction. All commands may address questions and submit changes to this instruction to N62.

19. Records Management. Records created as a result of this instruction, regardless of media and format shall be managed per SECNAV Manual 5210.1 of January 2012.

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

Scott Starkey
S. B. STARKEY
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

DEFINITIONS

The CNATRA Cyber IT/CSWF Qualification Program does not introduce terminology not already defined in references (a) through (i). Some terms and respective definitions are included below for ease of use and understanding.

Authorized User: Requires general computer skills and baseline understanding of CS to conduct work that is not IT or CS focused. The general DON workforce (military, civilian, and contractor) are authorized users.

Core Cyber IT/CS User: An authorized user (military, civilian, or contractor) who requires KSAs in both technical and managerial aspects of Cyber IT/CS. The Core User group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and IS.

Cybersecurity Workforce (CSWF): Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of CS into all aspects of engineering and acquisition of cyberspace capabilities.

Cyber IT/Cybersecurity Workforce Program Manager (Cyber IT/CSWF-PM): The Cyber IT/CSWF-PM is responsible for the administration of organization's CSWF Program. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization.

Cyberspace Information Technology Workforce: Personnel, who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments, architect, and engineer, acquire, implement, evaluate, and dispose of IT and services; as well as information resources management, and the management, storage, transmission, and display of data and information.

Defense Civilian Personnel Data System (DCPDS): The DCPDS is a human resources transaction and information system that supports civilian personnel operations in the DOD. The DCPDS is designed to support appropriated fund, non-appropriated fund, and local national human resources operations. DCPDS data elements shall be used to document and track civilian personnel information in support of requirements of this Directive.

Enhanced User: An authorized user (military, civilian or contractor) who requires detailed knowledge of Cyber IT and/or CS to support work in the development, maintenance, or operation of DON systems, including weapons, tactical, electronic and electrical services, navigation, and engineering. Enhanced users possess advanced Cyber IT/CS knowledge and abilities centered on particular professional areas.

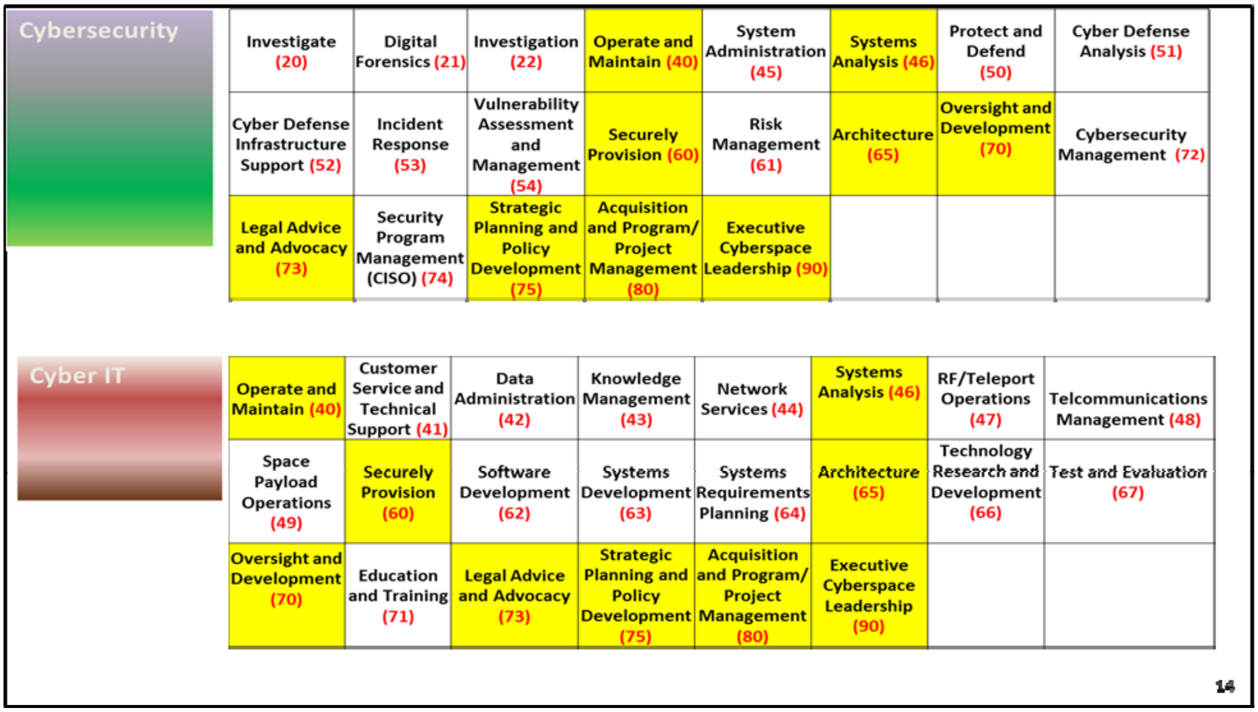
Personnel Qualification System (PQS): PQS is a qualification process for officer, enlisted, government civilians, and contract civilian personnel and is used when certification to a minimum level of competency is required prior to qualifying to perform specific duties.

Privileged Access: An authorized user who has access to system control, monitoring, administration, and criminal investigation or compliance functions. Privileged access is granted to a user who configures and operates IT within the authorities vested in them according to DON CS policies and procedures.

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Privileged Users operate IT within the authorities vested in them according to DON CS policies and procedures.

Qualified: An individual is considered qualified when he or she has met all of the conditions for "Trained" and completed the position relation OJT and JQR/PQS. This includes written designation by the appropriate command personnel.

DON CYBER IT/CSWF WORKFORCE CATEGORY MODEL AND CNATRA ASSIGNED SPECIALTY CODES



Cybersecurity

Investigate (20)	Digital Forensics (21)	Investigation (22)	Operate and Maintain (40)	System Administration (45)	Systems Analysis (46)	Protect and Defend (50)	Cyber Defense Analysis (51)
Cyber Defense Infrastructure Support (52)	Incident Response (53)	Vulnerability Assessment and Management (54)	Securely Provision (60)	Risk Management (61)	Architecture (65)	Oversight and Development (70)	Cybersecurity Management (72)
Legal Advice and Advocacy (73)	Security Program Management (CISO) (74)	Strategic Planning and Policy Development (75)	Acquisition and Program/ Project Management (80)	Executive Cyberspace Leadership (90)			

Cyber IT

Operate and Maintain (40)	Customer Service and Technical Support (41)	Data Administration (42)	Knowledge Management (43)	Network Services (44)	Systems Analysis (46)	RF/Teleport Operations (47)	Telecommunications Management (48)
Space Payload Operations (49)	Securely Provision (60)	Software Development (62)	Systems Development (63)	Systems Requirements Planning (64)	Architecture (65)	Technology Research and Development (66)	Test and Evaluation (67)
Oversight and Development (70)	Education and Training (71)	Legal Advice and Advocacy (73)	Strategic Planning and Policy Development (75)	Acquisition and Program/ Project Management (80)	Executive Cyberspace Leadership (90)		

14

The Cyber IT/CSWF Qualification Matrix details the Cyber IT/CSWF fundamentals and systems approved training, education and certifications by specialty area and proficiency level. It also details continuing education requirements. Cyber IT/CSWF PM will inform personnel as to which specialty area/s and watch stations/workstations they are to qualify for and in what order. Below are CNATRA's approved Specialty Area (SA) Codes.

SA Code	Title	SA Code	Title
41	Customer Service and Tech. Support	66	Technology Research and Dev.
42	Data Administration	67	Test and Evaluation
45	System Administration	72	Cybersecurity Management
46	System Analysis	74	Security Program Management
61	Risk Management	75	Strategic Planning and Policy Dev.
64	Systems Requirements Planning	90	Executive Cyberspace Leadership

INDIVIDUAL DEVELOPMENT PLAN

1. Requirement

Department of Defense Instruction (DoDI) 1400.25, Volume 410 (DoD Civilian Personnel Management System: Training, Education, and Professional Development) mandates that all DOD civilians have an Individual Development Plan (IDP). Additionally, SECNAVINST 1543.2 mandates that all Cyber IT/CSWF personnel have an IDP.

2. Overview

An IDP is used to identify learning and training needs, assess professional strengths and weaknesses, and budget the resources required to meet developmental goals. The IDP serves as a tool to help develop talent, expand employees' capabilities and over a period of time, build successful careers. Designed to promote more holistic thinking, the IDP is viewed as an investment strategy that helps sustain personal and career growth while inspiring progress toward career goals.

3. What is an IDP?

An IDP is defined as a written document used to help employees plan and chart their aspirations for career development that extends beyond their current needs and roles. The IDP provides the employee an opportunity to identify career objectives and knowledge; skills and abilities (KSAs) needed to be successful in his/her career. It is a tool used to aid an employee and the supervisor in creating a plan to support the individual's and the command's needs.

The IDP is used to:

a. Introduce short to long-term goals, assess strengths and weaknesses and plan more effectively for accomplishing career goals.

b. Identify required training and learning needs.

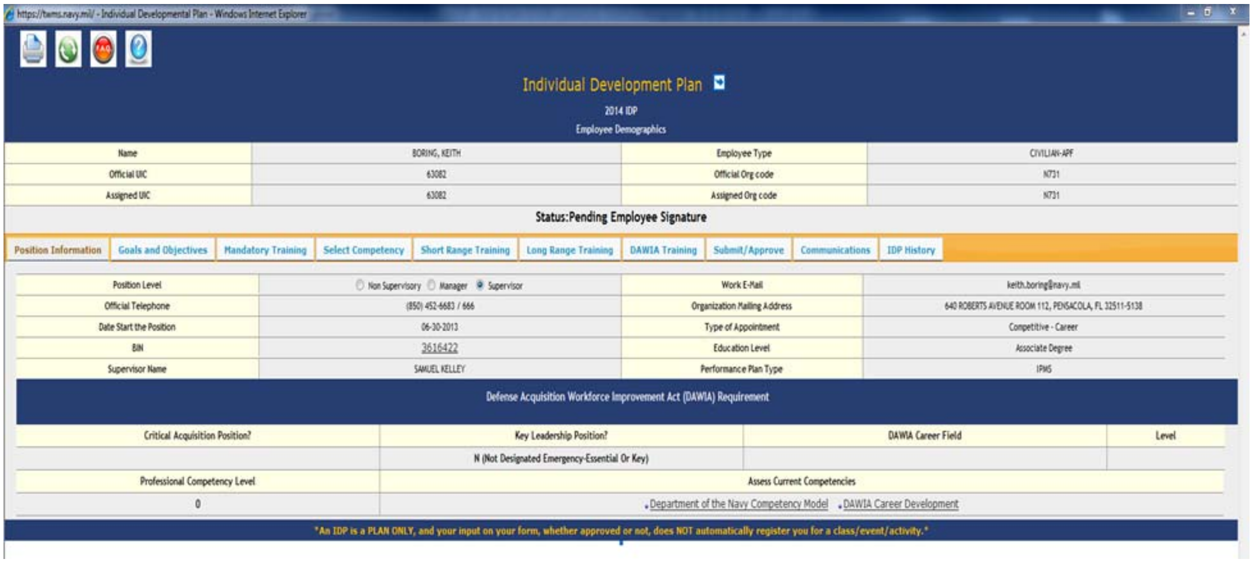
c. Improve job performance and enhance career opportunities.

d. Increase KSAs.

e. Serve as a documented record and a developmental agreement for recording any agreed upon developmental activities and other plans.

f. Coordinate and document planned training, annual continuing education/training and other related developmental experiences and assist in budgeting and scheduling resources.

IDPs are required to be updated annually. CNATRA requires the IDP to be located within Total Workforce Management System (TWMS).



Individual Development Plan

2014 IDP

Employee Demographics

Name	BORING, KEITH	Employee Type	CIVILIAN-APF
Official UIC	63082	Official Org code	N731
Assigned UIC	63082	Assigned Org code	N731

Status:Pending Employee Signature

Position Level	○ Non Supervisory ○ Manager ● Supervisor	Work E-Mail	keith.boring@navy.mil
Official Telephone	(850) 452-6683 / 666	Organization Mailing Address	640 ROBERTS AVENUE ROOM 112, PENSACOLA, FL 32511-5138
Date Start the Position	06-30-2013	Type of Appointment	Competitive - Career
BIN	3616422	Education Level	Associate Degree
Supervisor Name	SAMUEL KELLEY	Performance Plan Type	IPMS

Defense Acquisition Workforce Improvement Act (DAWIA) Requirement

Critical Acquisition Position?	Key Leadership Position?	DAWIA Career Field	Level
	N (Not Designated Emergency-Essential Or Key)		

Professional Competency Level	Assess Current Competencies
0	• Department of the Navy Competency Model • DAWIA Career Development

An IDP is a PLAN ONLY, and your input on your form, whether approved or not, does NOT automatically register you for a class/event/activity.

4. Total Workforce Management Services IDP Template

The TWMS IDP Template is located in TWMS at https://twms.navy.mil/selfservice/. Items that must be included in CNATRA IDPs:

a. 40 hours per year of approved Cyber IT/CSWF scoped continuous learning.

b. Training to initially meet requirements of billet assigned if not held by billet incumbent (these training hours are part of the continuing education unit (CEU) requirement).

c. Training to maintain Cyber IT/CSWF credential (these training hours are part of CEU requirement).

d. Training/qualification events for career growth (these training hours are part of CEU requirement).

WEB LINKS TO REFERENCES

DOD 8140.01 DOD Cyberspace Workforce Management, 11August2015
www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

DOD 8570.01-M DOD Information Assurance Workforce Improvement Program, 19December2005 with incorporated Change 4 dated November 10, 2015
www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

OPNAVINST 5239.1C Navy Information Assurance (IA) Program, 20August2008
https://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.1C.pdf

SECNAVINST 1543.2 Cyberspace/Information Technology Workforce Continuous Learning, 30November 2012
https://doni.daps.dla.mil/Directives/01000%20Military%20Personnel%20Support/01-500%20Military%20Training%20and%20Education%20Services/1543.2.pdf

SECNAVINST 5239.3C Department of the Navy Cybersecurity Policy, 2May2016
https://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3C.pdf

SECNAVINST 5239.20A Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, 10February 2016
https://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.20A.pdf

SECNAV M-5239.1 Department of the Navy Information Assurance Manual, November 2005
https://doni.daps.dla.mil/SECNAV%20Manuals1/5239.1.pdf

SECNAV M-5239.2 Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Program, June 2016
https://doni.daps.dla.mil/SECNAV%20Manuals1/5239.2%20(2016).pdf

SECNAV M-5510.36 Department of the Navy Information Security Program, June 2006
https://doni.daps.dla.mil/SECNAV%20Manuals1/5510.36.pdf