Department of Defense
MANUAL

NUMBER 3305.09
May 27, 2014

USD(I)

SUBJECT: Cryptologic Accreditation and Certification

References: See Enclosure 1

1. PURPOSE. This manual:

a. Provides accreditation guidance and procedures for DoD education and training institution(s) (referred to in this manual as "institutional accreditation") that support the cryptologic community in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)) and the policy in DoD Instruction (DoDI) 3115.11 (Reference (b)).

b. Provides guidance and procedures for developing and implementing certification programs in accordance with Reference (b).

c. Implements the policy in DoDI 3305.09 (Reference (c)) and establishes roles and assigns responsibilities for the development, implementation, and maintenance of the cryptologic certification program for training and developmental purposes in accordance with Reference (b).

2. APPLICABILITY. This manual applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this manual as the "DoD Components").

3. RESPONSIBILITIES. See Enclosure 2.

4. PROCEDURES

a. Enclosure 3 establishes responsibilities for the Associate Director for Education and Training (ADET).

b. Enclosure 4 identifies the accreditation requirements used to support the cryptologic community and the cryptologic certification program.

c. Enclosure 5 identifies the procedures for developing the accreditation-ready cryptologic certification program. This includes guidelines for:

(1) Developing, documenting, overseeing implementation of, and maintaining criteria for identifying and coding cryptologic functions, positions, or work roles addressed by the cryptologic certification program.

(2) Establishing formal and documented processes for assessing and evaluating whether personnel within the cryptologic workforce have acquired the knowledge and skills required to perform cryptologic functional tasks.

(3) Categorizing cryptologic functions, positions, or work roles in terms of the cryptologic functional tasks and identifying certifications applicable to personnel performing the cryptologic functional tasks.

d. Enclosure 6 provides templates for preparation of accreditation documentation.

5. INFORMATION COLLECTION REQUIREMENTS. The Annual Report of Intelligence and Security Training, Education, and Certification, referred to in paragraph 5d of Enclosure 2, paragraph h(5) of Enclosure 3, and section 6 of Enclosure 5 of this manual, has been assigned report control symbol DD-INT(A)2252 as prescribed in DoD Manual 3305.02 (Reference (d)).

6. RELEASABILITY. **Unlimited**. This manual is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This manual:

a. Is effective May 27, 2014.

b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoDI 5025.01 (Reference (e)).

c. Will expire effective May 27, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (e).

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. NSA/CSS ADET
4. Accreditation Requirements and Standards
5. Cryptologic Certification Program Procedures
6. Templates for Consistent Documentation

Glossary

TABLE OF CONTENTS

TABLES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(b) DoD Instruction 3115.11, "DoD Intelligence Human Capital Management Operations," January 22, 2009, as amended
(c) DoD Instruction 3305.09, "DoD Cryptologic Training," June 13, 2013
(d) DoD Manual 3305.02, "DoD Collection Management (CM) Accreditation and Certification," November 21, 2012
(e) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended
(f) DoD Directive 1322.18, "Military Training," January 13, 2009
(g) DoD Instruction 1400.25, Volume 250, "DoD Civilian Personnel Management System: Volume 250, Civilian Strategic Human Capital Planning (SHCP)," November 18, 2008
(h) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013
(i) Intelligence Community Directive Number 610, "Competency Directories for the Intelligence Community Workforce," September 1, 2008, as amended
(j) Institute for Credentialing Excellence, "National Commission for Certifying Agencies: Standards for the Accreditation of Certification Programs," September 2004
(k) Institute for Credentialing Excellence, "ICE 1100 2010(E) – Standard for Assessment-Based Certificate Programs," 2009[1]
(l) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004
(m) Society for Industrial and Organizational Psychology, Inc., "Principles for the Validation and Use of Personnel Selection Procedures," 4th Edition (2003)
(n) American Educational Research Association, American Psychological Association, and National Council on Measurement in Education, "Standards for Educational and Psychological Testing," 1999[2]
(o) Section 300.103(c) of Title 5, Code of Federal Regulations
(p) Chapter 126 of Title 42, United States Code (also known as "The Americans with Disabilities Act of 1990")
(q) Intelligence Community Directive Number 652, "Occupational Structure for the Intelligence Community Civilian Workforce," April 28, 2008

[1] Available for purchase at http://www.credentialingexcellence.org/p/cm/ld/fid=15
[2] Available for purchase at http://www.aera.net/tabid/11736/Default.aspx

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I):

a. Exercises the approval authority for the cryptologic certification program for externally accredited certifications as described in Enclosure 4 of this manual.

b. Ensures sustainment requirements of the cryptologic certification program and institutional accreditation, as required to satisfy the DoD Components' implementation plans and in accordance with Reference (b), are identified and included in Planning, Programming, Budgeting, and Execution (PPBE) actions.

c. Reviews cryptologic certification program resource requests upon budget submission, and provides additional guidance as needed.

d. Ensures cryptologic education and training institutions are compliant with the requirements described in Enclosure 4 of this manual.

e. Accepts and approves certification conferral recommendations for externally accredited certification programs.

f. Coordinates competency and certification programs with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)).

g. Ensures the DoD Component heads determine certification requirements for military, civilian and contractor manpower, and contract support for cryptologic-related mission support and force structure, as required.

h. In coordination with the USD(P&R), has primary responsibility for management and program review of individual, collective, and staff training for cryptologic skills in accordance with Reference (c) and DoDD 1322.18 (Reference (f)).

2. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), the DIRNSA/CHCSS:

a. In accordance with Reference (c), appoints the National Security Agency/Central Security Service (NSA/CSS) ADET as the principal executive for all cryptologic certification program matters related to education, training, and professional development.

b. In accordance with Reference (b), appoints the NSA/CSS Associate Director for Human Resources (ADHR) as the principal executive responsible for high stakes decisions associated with positions:

(1) All cryptologic certification program matters related to decisions regarding the selection of external applicants for civilian positions.

(2) Placement of external applicants and current employees into civilian positions or particular civilian pay schedules.

(3) Promotion of current civilian employees from one grade to another.

3. USD(P&R). The USD(P&R):

a. Incorporates cryptologic certification designations into USD(P&R) management of civilian cryptologic professionals.

b. Captures and incorporates certification data in personnel and manpower databases under USD(P&R) authority.

c. Incorporates progress in meeting cryptologic goals into the strategic human capital planning (SHCP) and congressional reports in accordance with Volume 250 of DoDI 1400.25 (Reference (g)).

d. In coordination with the USD(I), has primary responsibility for management and program review of individual, collective, and staff training for cryptologic skills in accordance with References (c) and (f).

4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) implements the requirements of this manual, as appropriate, for the acquisition of services in support of cryptologic services in accordance with DoDI 5000.02 (Reference (h)).

5. DoD COMPONENT HEADS AND COMMANDANT, U.S. COAST GUARD. The DoD Component heads and the Commandant, U.S. Coast Guard:

a. Implement policies, procedures, programs, and requirements as specified in this manual for the implementation of the cryptologic certification program.

b. Identify applicable certifications for their respective DoD Component's military, civilian and contractor cryptologic functions, positions, or work roles in terms of cryptologic functional tasks.

c. Implement applicable certifications for their respective DoD Component's military, civilian and, when applicable, contractors tasked to perform cryptologic functions or work roles.

d. Develop specific input related to the cryptologic certification program for inclusion in its respective DoD Component's Annual Report on Accreditation and Certification and submit to the NSA/CSS ADET for reporting to the USD(I) and to the SHCP Program Office for incorporation into the DoD SHCP.

e. Support the continuous improvement of the cryptologic certification program by submitting recommendations to the NSA/CSS ADET regarding DoD Component-specific needs or issues that affect the effective implementation of each relevant cryptologic certification program and recommended adjustments including, but not limited to, additions, deletions, or changes to the certification framework, certification blueprints, or certification scheme.

f. Identify cryptologic certification program education, training, and certification renewal standards including associated costs for time required for professional development, and include in PPBE actions.

g. Fund the development, implementation, and maintenance costs for each approved DoD Component-specific cryptologic certification program and associated education and training programs.

h. Review and coordinate the candidate lists with the Cryptologic Certification Administrative Program Office prior to submission to the NSA/CSS ADET for NSA/CSS for conferral recommendations of relevant certifications.

i. Provide subject matter experts to support cryptologic certification projects, committees, and initiatives.

j. Ensure DoD Component-level cryptologic education and training institutions are accredited and sustained in accordance with Enclosure 4 of this manual.

ENCLOSURE 3

NSA/CSS ADET

The NSA/CSS ADET is the principal executive and training director for all cryptologic certification program matters related to education, training, and professional development. The NSA/CSS ADET:

a. Determines requirements for developing and establishing NSA/CSS and externally accredited cryptologic certification programs.

b. Documents, oversees implementation of, and maintains a requirements-driven system for the cryptologic certification program. The system will identify the cryptologic functions, positions, or work roles that will be addressed by a cryptologic certification program and determine which approved cryptologic certification programs will be submitted for externally accredited based on the accreditation and certification standards set forth in this manual.

c. Identifies and documents the knowledge and skills associated with functional tasks, informs the Office of the USD(P&R) of competency requirements, and ensures that:

(1) The cryptologic community knowledge and skills are aligned with the directory contained in Intelligence Community Directive (ICD) Number 610 (Reference (i)).

(2) The cryptologic community-defined, requirements-based functional tasks are defined in accordance with Reference (c) and vetted through mission elements with criteria established by the cryptologic community.

(3) Cryptologic certification program information verifies, validates, and is updated to reflect mission, policy, doctrine, tactics, techniques, and procedure changes.

d. Submits all externally accredited cryptologic certification programs to the USD(I) for approval.

e. Identifies resource requirements for each cryptologic certification program and considers for inclusion in the NSA/CSS budget.

f. Establishes a certification administrative program office that supports the implementation and maintenance of each cryptologic certification program.

g. Implements and maintains cryptologic education and training opportunities that allow cryptologic personnel to acquire knowledge and skills identified by the cryptologic certification program.

h. Identifies and documents the specific implementation and sustainment requirements for each cryptologic certification program, as specified in this manual.

(1) Establishes and implements policies and procedures for each cryptologic certification program.

(2) In coordination with the DoD Component review the candidate list(s) to be submitted by the Certification Administrative Program Office before submission for conferral of certifications.

(3) Establishes and coordinates a process for developing, reviewing, and endorsing each DoD Component's Annual Report on Accreditation and Certification specific to the cryptologic certification program.

(4) Establishes and implements a process for disseminating information about the cryptologic certification program.

(5) Designs, develops, and implements a plan for evaluating the efficiency and effectiveness of the cryptologic certification program and collects relevant metrics for each cryptologic certification within the program for inclusion in the Cryptologic Training Council (CTC) annual report to the USD(I).

i. Applies for external accreditation as described in Enclosure 4 of this manual, when applicable.

j. Reviews certification conferral recommendations for each cryptologic certification program and submits names to the USD(I) for externally accredited certification conferrals.

k. Coordinates with the NSA/CSS ADHR on the proposed uses of the cryptologic certification program. When the cryptologic certification program is to be used for high stakes decisions, NSA/CSS ADHR will ensure that the certifications have been developed, validated, and maintained in compliance with relevant laws, policies, and professional practice guidelines for their intended use and that the proposed application of the cryptologic certification program is appropriately aligned with the agency's civilian human resources policies, programs, and procedures.

ENCLOSURE 4

ACCREDITATION REQUIREMENTS AND STANDARDS

1. INTRODUCTION. Accreditation applies to defense education and training institutions and the cryptologic certification program. Accreditation assures the quality of the institution or certification program and assists in the improvement of the institution or certification program.

2. ACCREDITATION FOR INSTITUTIONS

a. Bodies that conduct institutional accreditation are national or regional in scope and consider the characteristics of whole institutions. An institutional accrediting body gives attention not only to the offerings of the institutions it accredits, but to other institutional characteristics such as student personnel services, financial status, administrative structure, facilities, and equipment.

b. To be accredited, DoD institutions and programs must meet DoD Component published standards and the associated criteria of a U.S. Secretary of Education-recognized accrediting agency, such as the Council on Occupational Education.

c. Additional accreditation requirements may be required by the NSA/CSS ADET and/or the NSA/CSS ADHR; institutions sponsoring accreditation processes related to cryptologic certification initiatives must meet the standards and associated criteria developed and distributed by the NSA/CSS ADET and/or the NSA/CSS ADHR.

d. It is the responsibility of the DoD institution sponsoring the accreditation process to inform the accrediting organization of any security clearance requirements during the establishment of its candidacy.

3. ACCREDITATION FOR A CRYPTOLOGIC CERTIFICATION PROGRAM

a. Certifications designated by the NSA/CSS ADET and/or the NSA/CSS ADHR for external recognition and developed under the direction of this manual must be accredited and maintain accreditation to ensure quality as described in the Standards for the Accreditation of Certification Programs and the Quality Standard for Assessment-Based Certificate Programs (References (j) and (k)).

b. Accreditation of designated cryptologic certification programs must be achieved by meeting the published standards of the nationally recognized certification accreditation body, the National Commission for Certifying Agencies (NCCA). The application process and establishment of candidacy for NCCA accreditation is described in References (j) and (k).

4. PROFESSIONAL DEVELOPMENT STANDARDS

a. Achieving the cryptologic mission requires building and retaining an agile, highly skilled workforce that can respond flexibly to dynamic requirements. Building this workforce requires two complementary components: workforce planning and professional development. Workforce planning entails analyzing the capabilities needed to achieve the current mission and forecasting the capabilities that are needed in the future. Current and future talent gaps can be addressed through a combination of staffing (e.g., hiring, contracting, or reassignment) and professional development programs.

b. Professional development is a comprehensive, sustained approach to acquiring or improving knowledge and skills to meet mission demands in one's current or future roles. One way to verify that cryptologic professionals have acquired the relevant knowledge and skills is through certification. In cases where certification has been determined the optimal assessment method, NSA/CSS is implementing a two-pronged approach, as defined in paragraphs 4b(1) and 4b(2) of this manual.

(1) National Security Agency (NSA) Cryptologic Certification Program. A NSA Cryptologic Certification Program is established when one segment of the cryptologic workforce is required to complete a consistent set of development activities and pass one or more standardized assessments. This program applies to functions, positions, or work roles under the purview of the Director, NSA/CSS. Each NSA Cryptologic Certification Program must include:

(a) A clear statement of the purpose of the program.

(b) A definition of the population to which the certification applies.

(c) A job analysis.

(d) Validated components for acquiring a certification to include but not limited to education, training, experience, and assessments.

(e) Assessment materials in accordance with test development standards.

(f) Implementation guidance and communications for the certification program.

(g) Ongoing management of the program.

(2) Externally Accredited Cryptologic Certification Programs

(a) Externally accredited cryptologic certification programs of DoD education and training institutions include national-level certifications that meet the accreditation criteria established by NCCA.

(b) External recognition is required when a cryptologic certification program applies to more than one workforce segment (e.g., in addition to NSA/CSS civilian or military personnel,

the certification requirements may also apply to personnel who are assigned to a cryptologic function, position, or work role addressed by a cryptologic certification program and under the purview of a Military Department, a Combatant Command, and/or an Intelligence Community (IC) element).

(c) The externally accredited cryptologic certification programs prepare such personnel for duty within other departments, agencies, and elements of the IC consistent with section 1041 of Public Law 108-458 (Reference (l)). An externally accredited cryptologic certification program must include:

1. A clear statement of the purpose of the program.

2. A definition of the population to which the certification applies.

3. A job analysis.

4. Validated components for acquiring a certification to include but not limited to education, training, experience, and assessments.

5. Assessment materials in accordance with test development standards.

6. Implementation guidance and communications for the certification program.

7. Ongoing management of the program.

8. Documentation that the program meets the external accreditation criteria established by NCCA.

c. Responsibilities for both the NSA Cryptologic Certification Program and the externally accredited cryptologic certification program that have been approved by the NSA/CSS ADET and/or NSA/CSS ADHR will include articulated professional development standards codified by the professional development plans and associated documentation described in this enclosure. A cryptologic certification program development lead will be identified with the authority and responsibility for documenting and implementing each approved cryptologic certification and will:

(1) Be responsible for coordinating with the NSA/CSS ADET Certification Program Management Office on all aspects of the approved cryptologic certification program.

(2) Ensure the appropriate professional development plans and associated documentation adhere to the standards set forth in this enclosure to include a clear description of the population impacted by the plan.

(3) The alignment of Reference (i) competencies and certification levels within the target population will be documented. An implementation plan will ensure the professional development plan is properly resourced and sustainable.

d. Professional development plans will specify learning and development strategies for each target population. Primary components for these strategies should include:

(1) Developmental Activity Linkage. Developmental activities should be mapped to competencies at each work level and at each proficiency level. Guidelines to be used are:

(a) Determine which competencies should be linked to a given activity. A linkage may be made if the knowledge and skills associated with the activity are reflected in the competency definition.

(b) Determine which activities should be used to meet the standards established in the job task analysis by comparing the competencies.

(2) Assessments and Testing

(a) Standardized assessments should be used to evaluate knowledge and skills gained through a specific activity or group of activities.

(b) All validated training courses will include an appropriate standardized test or assessment of knowledge and skills so that a minimum level of competence is assured for those completing a course. Where possible, the same or similar assessments should be used for similar courses in different IC elements to facilitate establishing the equivalency of courses.

(c) Tests and assessments should be developed by following professional standards and the process needs to include establishing evidence for the reliability and validity of the assessment for those courses requiring a high rigor assessment.

(3) Developmental Paths

(a) A developmental path specifies a recommended sequence of learning and developmental activities linked to work or career levels that can be used to guide employees in choosing the right activities at the right stages in their career to meet requirements.

(b) When individual development plans are established, the planned activities should clearly link to addressing mission requirements and be consistent with achieving the developmental activities and milestones specified in relevant developmental paths.

(c) Table 1 lists the internal and external participants required for the development and implementation process for each level of desired outcome. Minimum requirements for developmental paths include:

1. A sequence of job roles and levels that provides one or more developmental paths within a given occupation or specialty.

2. The core activities performed in each major job role at each work level and the competencies required to perform successfully.

3. The developmental activities that link to the competencies for each major job role at each work level along with specification of whether these activities are mandatory or optional.

Table 1. Outline of Professional Development and Certification Standards

	Link Development Activities to Competencies and Proficiencies	Assessed Development Activities	Developmental Paths	NSA Cryptologic Certification Program	Externally Accredited Cryptologic Certification Program
Level of Effort for Organizational Subject Matter Experts and Certification Program Management	Low – Requires input from a small number of subject matter experts.	Medium – Requires construction of a test or other assessment tool and resources to complete assessments.	Medium – Requires input from subject matter experts from across work levels and related jobs.	High – Requires a rigorous process, the involvement of multiple groups of subject matter experts, and significant resources to implement.	Highest – Requires a rigorous process, the involvement of multiple groups of subject matter experts, and significant resources to meet established external accreditation requirements and review from experts.
Assurance of Competency Mastery	Low – Participation in the development activity does not guarantee skill acquisition.	Medium – Results in an objective assessment of actual proficiency limited to content covered in the activity.	Medium – A map serves as a valuable guide for gaining knowledge and skills but does not guarantee desired skill acquisition.	High – This process ensures the program builds required skills involving standardized assessment of individuals' skills.	High – This process ensures the program builds required skills involving standardized assessment of individuals' skills.
Accreditation or Validation Process	Subject Matter Experts and Instructional Design Professionals	Subject Matter Experts, Curriculum Managers, Skill Community Directors, Instructional Design and Testing Professionals	Subject Matter Experts, Curriculum Managers, Skill Community Directors, Instructional Design Professionals	Human Resource Professionals, Subject Matter Experts, Curriculum Managers, Skill Community Directors and Advocates, Testing and Assessment Professionals	Human Resource Professionals, USD(I), Subject Matter Experts, Testing and Assessment Professionals, NCCA

5. DoD INSTRUCTOR CERTIFICATION STANDARD

a. Purpose

(1) In addition to meeting the standards for institutional accreditation, certification program accreditation, and development of quality professional development programs, institutions responsible for the delivery of the highest quality of instruction must also meet the instructor standards established in the DoD Instructor Certification Standard. This standard establishes standards for basic instructor certification to ensure fully competent learning facilitators conduct all education and training.

(2) The standard provides a basic framework for the development and certification of instructors within the training and education enterprise to complement existing NSA/CSS instructor development and certification programs. This standard applies to all instructors and faculty within the training and education components subject to the provisions of Reference (b).

b. Responsibilities. The DoD Instructor Certification Standard establishes general guidelines for basic instructor development, evaluation, and certification. The standard supplements policy that may already be in place within the respective education and training institutions.

c. Oversight of the Standard

(1) To assure alignment of the education and training institutions to these standards, and to encourage best practices among all learning institutions, the USD(I) conducts biennial staff assistance visits (SAVs) with each institution.

(2) The results of these SAVs will be shared with all education and training institutions to track the progress of each school in meeting these standards and leverage the best employed practices to meet these standards for the mutual benefit of all institutions.

ENCLOSURE 5

CRYPTOLOGIC CERTIFICATION PROGRAM PROCEDURES

1. CRYPTOLOGIC CERTIFICATION PROGRAM OBJECTIVES. The cryptologic certification program:

a. Promotes a common and shared understanding of the criteria and the policies and procedures for applying those criteria in determining which cryptologic functions, positions, or work roles will be addressed by the cryptologic certification program.

b. Promotes a common and shared understanding of the certification requirements for identified and coded cryptologic functions, positions, or work roles; and the policies and procedures for developing and validating those requirements.

c. Promotes an interoperable cryptologic workforce by establishing uniform processes for assessing, evaluating, and determining whether a workforce member has met defined certification requirements applicable to identified and coded cryptologic functions, positions, or work roles.

d. Certifies that cryptologic personnel (military, civilian, and contractor) possess the knowledge and skills associated with the competencies necessary to successfully carry out the applicable cryptologic functional tasks.

e. Facilitates sound professional development, education, and training by ensuring, through a formal evaluation process, that such professional development, education, and training programs provide individuals the opportunity to acquire the documented cryptologic essential body of knowledge.

2. ESTABLISHING CRYPTOLOGIC CERTIFICATION PROGRAMS

a. NSA and externally accredited cryptologic certification programs are approved through the NSA/CSS ADET and in partnership with the NSA/CSS ADHR. NSA and externally accredited cryptologic certification programs will formally recognize, through the conferral of NSA/CSS-sponsored certification credentials, cryptologic personnel's mastery of knowledge and skills critical to the successful performance of functional tasks associated with identified and coded cryptologic functions, positions, or work roles.

b. A cryptologic certification program meeting the requirements for external accreditation is submitted to the USD(I) for approval. The externally accredited cryptologic certification program will formally recognize, through the conferral of USD(I)-sponsored certification credentials, cryptologic personnel's mastery of knowledge and skills critical to the successful performance of functional tasks associated with identified and coded cryptologic functions, positions, or work roles.

c. Supporting documentation for each cryptologic certification will be included in a cryptologic certification program design document (PDD). For the externally accredited cryptologic certification program, a PDD will include documentation requirements as required by Reference (j). At a minimum, a PDD will include:

(1) Purpose, governance, and resources.

(2) Responsibilities to stakeholders.

(3) Assessment instruments.

(4) Renewal.

d. Each certification program's success hinges on the valid identification of the essential body of knowledge required to successfully perform an identified and coded cryptologic function, position, or work role; a rigorous analysis and identification of the segment of that essential body of knowledge addressed through the certification process; and the integrity of the assessment and evaluation processes the program uses to determine mastery. Each PDD documents the process and applicable policies and procedures providing stakeholders visibility into the strategic, operational, and technical elements of a certification program.

3. STANDARDS FOR ESTABLISHING FORMAL PROCESSES FOR CREDENTIALING CRYPTOLOGIC PERSONNEL. The success of a certification program depends on the psychometric integrity of the assessment and evaluation processes the program uses. For those cryptologic certification programs that meet the criteria for external accreditation, Reference (j) provides the accreditation standards the cryptologic certification program must meet to ensure these processes result in reliable information to make valid certification conferral decisions.

a. The analytical method employed to catalogue the requisite knowledge and skills must comply with applicable legal, professional, and technical guidelines in accordance with Reference (g), Principles for the Validation and Use of Personnel Selection Procedures (Reference (m)), Standards for Educational and Psychological Testing (Reference (n)), and part 300.103(c) of Title 5, Code of Federal Regulations (Reference (o)).

b. Only the assessment strategies included and described in paragraph 4.c.(2) of this Enclosure will be used as a basis for certifying cryptologic personnel. Use of these strategies must be supported by documented validity evidence in accordance with References (m), (n), and (o).

c. To ensure that the USD(I) and the NSA/CSS ADET can make valid certification conferral decisions based on information resulting from chosen assessment strategies, implementation of these strategies must comply with applicable legal, professional, and technical guidelines in accordance with References (m), (n), and (o).

4. ELEMENTS OF A CERTIFICATION PROGRAM FOR CREDENTIALING CRYPTOLOGIC PERSONNEL. The formal processes used during the formation of the cryptologic certification elements are captured in the certification framework, certification blueprint, and certification scheme.

a. Certification Framework. Each certification program will define a certification framework that meets the needs of the cryptologic community and is in accordance with the essential body of knowledge. The framework will be used to prepare notional developmental pathways.

(1) Each certification framework will array certification requirements in a manner that reflects the logical progression with which the cryptologic workforce will need to demonstrate acquisition of the essential body of knowledge.

(2) For externally accredited certifications, each certification framework will be modular to account for the variability with which DoD Components configure functions, positions, work roles, or billets to carry out functional tasks.

(3) Each certification program will address segments of the essential body of knowledge that are relevant and critical to cryptologic functional tasks. The intended audience will be the cryptologic workforce.

(4) If subsequent certifications are required, each will address segments of the cryptologic essential body of knowledge critical to the successful performance of defined categories of cryptologic functional tasks. Each certification framework will be aligned with ODNI-defined competency standards when available or within 1 year of release of updates in accordance with Reference (i).

b. Certification Blueprint. A blueprint is created for each certification specified in the framework. The blueprint identifies specific segments of the essential body of knowledge for each certification.

(1) The blueprint is reviewed, validated, and endorsed by the governance board responsible for the professional development standards relevant to the certification.

(2) The blueprint guides the selection of assessment processes.

(a) Assessment processes will be developed, validated, implemented, and maintained in accordance with applicable legal, professional, and technical guidelines and in accordance with References (m), (n), and (o).

(b) The development and validation of assessment processes will be documented in accordance with applicable legal, professional, and technical guidelines and in accordance with References (m), (n), and (o) and relevant accreditation standards in accordance with References (j) and (k).

c. Certification Scheme. Each program's certification scheme describes the set of assessment processes it will use to implement defined certification blueprints. It specifies a certification's eligibility requirements and prerequisites, certification assessment strategies, and its renewal requirements.

(1) Eligibility and Prerequisites. Each cryptologic certification will, when applicable, define specific prerequisites cryptologic personnel must meet to be considered eligible candidates for that certification. Prerequisites may include:

(a) Verification that a member is part of the cryptologic workforce.

(b) Attainment of a relevant, lower-level cryptologic certification, when applicable.

(c) Successful completion of education and training courses or programs that are required but not part of the certification's assessment strategies.

(2) Assessment Strategies. Each cryptologic certification program will specify assessment strategies for each certification, which are documented in the certification framework. Assessment processes, established in assessment strategies, will provide evidence that candidates for certification possess the essential body of knowledge. Assessment strategies may include:

(a) Education and Training. Assessment processes may include successful completion of courses or programs that cover targeted competencies. To be part of the assessment strategies, courses or programs will:

1. Go through a formal review or development process that ensures they cover competencies specified in the cryptologic certification standards.

2. Publish learning objectives associated with the targeted competencies specified in the cryptologic certification standards.

3. Use assessments that meet the appropriate validity and reliability standards to gauge the extent to which students have acquired the targeted competencies they cover.

4. Meet all assessment-based certification accreditation standards in accordance with Reference (k).

(b) Accomplishment Records. Assessment processes may include evaluations of accomplishments and experiences that reflect the successful application of targeted competencies to carry out applicable cryptologic functional tasks. To be part of the assessment strategies, evaluations of accomplishments and experiences will:

1. Use structured, standardized, and formalized processes for collecting and evaluating accomplishments and experiences.

2. Be based on verifiable and verified accomplishments and experiences within a given time frame.

3. Be conducted by professionals trained in effective evaluation of such assessment strategy.

(c) Work Products. Assessment processes may include evaluations of work products that reflect the successful application of targeted competencies to carry out applicable cryptologic functional tasks. To be part of the assessment strategies, evaluations of work products will:

1. Use explicit and community-accepted quality criteria or standards.

2. Use structured, standardized, and formal evaluation processes.

3. Be conducted by professionals trained in effective evaluation of such assessment strategy.

(d) Standardized Assessments. Assessment processes may include successful exhibition of knowledge and skills using standardized assessments that measure the knowledge and skills associated with the targeted competencies.

(e) Reuse of Assessments. When applicable, different certifications targeting the same set of competencies will use the same assessment process to evaluate cryptologic workforce attainment of those competencies.

(3) Certification Renewal. Certification renewal consists of maintenance and recertification.

(a) Maintenance. Each cryptologic certification program will identify certification requirements for maintenance of the cryptologic workforce certification status. Certification maintenance requirements are defined in terms of professional development and continuing education using hours, units, or credits.

(b) Recertification. Each cryptologic certification program will define recertification policies and procedures for each certification. This includes:

1. Conditions and events that will trigger the need for certification holders to go through a recertification process.

2. Elements of the original assessment strategies that certification holders must meet in order to be recertified.

(4) Adjudication. In accordance with Reference (j), each cryptologic certification program will confer certifications only to those cryptologic personnel who meet all of the applicable requirements. Each cryptologic certification program will also define actions available to individuals who do not meet the certification requirements to include:

(a) The amount of time cryptologic personnel must wait before they are eligible to re-apply for failed elements of the certification.

(b) Policies and procedures for appeals.

d. Documentation of Each Certification Program for Credentialing Cryptologic Personnel. Each cryptologic certification program will document policies and procedures in its respective PDD.

5. CERTIFICATION ADMINISTRATIVE PROGRAM OFFICE. The functions of the Certification Administrative Program Office include:

a. Management of Certification Conferral Process. In coordination with the cryptologic governance structure and the NSA/CSS ADET, submit names for conferral. Dissemination of information to the DoD Components will flow from the Certification Administrative Program Office in accordance with their implementation plan. Supporting documentation is included in each PDD.

b. Maintenance of Applications, Records Management, and Documentation. Establish and provide eligible candidates an application process for certification that is administered in a consistent, accessible, and secure manner and complies with the guidelines and procedures outlined in this manual. Maintain security of candidate records, scores, and certification and decertification documents. Track candidates from initial request to certification and report information to the DoD Components, when applicable. Supporting documentation is included in each PDD.

c. Management of Certification Tests, Tools, and Protocols and Oversight of Their Delivery. Establish procedures to manage the tests, tools, and protocols. Certification testing will be administered in an approved, proctored environment, using standardized procedures and in compliance with applicable laws, including chapter 126 of Title 42, United States Code (also known as "The Americans with Disabilities Act of 1990" (Reference (p)), and external accreditation standards. Supporting documentation is included in each PDD.

d. Management of Appeals. Candidates have the right to appeal all decisions relating to their eligibility evaluation as well as their cryptologic certification examination results. All appeals must be in writing and submitted to the cryptologic governance structure within 90 days of being notified of their ineligibility to be certified. Candidates must identify the reasons for the appeal. The appeals process will be administered in a manner consistent with an approved appeals process designed by the cryptologic governance structure. Supporting documentation is included in each PDD.

e. Management of Human Resources. The Certification Administrative Program Office will be staffed with personnel who possess credentials consistent with their responsibilities. Supporting documentation is included in each PDD.

f. Management of Data. Establish and implement policies and procedures necessary to protect and secure confidential personnel certification data including, but not limited to, personnel records, tests, and statistical data. These policies and procedures will clearly define and establish "need to know" criteria and cryptologic-related system access requirements. Supporting documentation is included in each PDD.

6. COMPLETE ANNUAL REPORT ON ACCREDITATION AND CERTIFICATION. NSA/CSS and, as applicable, DoD Components will develop its respective Annual Report on Accreditation and Certification and submit to the CTC for inclusion in reports to the USD(I) in accordance with Reference (c). This report must include:

a. Implementation Plan. Describe the NSA/CSS plan for incrementally implementing this manual over a 5-year period.

b. Management Plan. Establish and maintain a systematic approach to track and monitor cryptologic certification program certification attainment, and maintenance for cryptologic functions, positions, or work roles included in each certification program and report staffing compliance.

7. IDENTIFICATION OF APPLICABLE CERTIFICATIONS FOR CRYPTOLOGIC FUNCTIONS, POSITIONS, OR WORK ROLES. The NSA/CSS ADET documents the requirements process for identification of applicable certifications. The requirements process will be based on cryptologic mission needs. The NSA/CSS Mission Resource Authorities and Deputy Chief Central Security Service will recommend functions, positions, or work roles which will be included in a certification program. Funding for development and sustainment of cryptologic certifications will be incurred by the requesting organization.

a. Cryptologic functions, positions, or work roles will be coded in the NSA/CSS Human Resource Database of Record and when appropriate, in the DoD Component database of record to identify the required certifications. Codes will be used to identify which cryptologic certification(s) will be applicable to specific functions, positions, or work roles. Steps to ensure proper coding include, but are not limited to:

(1) Identify cryptologic certification program requirements for identified and categorized cryptologic functions, positions, or work roles.

(2) Enter certification specialty codes into the NSA/CSS authoritative database of record for any personnel performing cryptologic functions for which a certification requirement has been approved.

(3) Enter certification classification as an additional skill identifier or military occupational specialty code into the military database for all military personnel performing cryptologic functions.

(4) If applicable, and approved by the NSA/CSS Associate Directorate for Human Resources for NSA civilian workforce members, establish and implement a "condition of employment" agreement for cryptologic personnel (military, civilian, and contractor) that states they will obtain the appropriate certifications for the functions, positions, or work roles that they fill. The agreement will also include a release for the DoD Components to have access to the individual's certification qualifications.

b. Attainment of a certification applicable to a cryptologic function, position, or work role does not confer to the certification holder an automatic right to fill that cryptologic function, position, or work role. DoD Components may levy additional requirements for staffing purposes and make final decisions regarding the staffing of their cryptologic functions, positions, or work roles.

c. Incumbents of cryptologic functions, positions, or work roles may not need to obtain certifications to perform in their current cryptologic functions, positions, or work roles, unless specified by Director, NSA/CSS, based on mission critical needs. See Glossary for definition of "incumbent."

d. Workforce members assigned to a function, position, or work role that requires a certification will achieve the appropriate certification within the time period specified within each PDD, typically within 2 years, unless identified as an incumbent by the DoD Component or at the discretion of the Director, NSA/CSS.

e. When applicable, new hire (military, civilian, and contractor) qualification periods begin on the first duty day assigned to the function, position, or work role. Vacancy announcements or job profiles must state certification requirements.

ENCLOSURE 6

TEMPLATES FOR CONSISTENT DOCUMENTATION

1. GENERAL. This enclosure provides templates for documenting certification programs in a PDD.

2. DOCUMENTATION OF A PDD. The following templates are provided for uniformity when presenting related accreditation and certification documentation.

a. Table 2 specifies the certification's target audience, the knowledge and skills identified to exhibit mastery, the assessment processes that define the assessment strategies, and the name of the certification credential.

Table 2. Certification Program Assessment Outline

TARGET AUDIENCE	EXHIBIT MASTERY	ASSESSMENT STRATEGIES	CERTIFICATION CREDENTIAL
Types of professionals performing functional tasks	Relevant knowledge and skills that make up competencies	Approved assessment processes	Certification Name

b. Each certification must detail the assessment strategies as specified in Table 2.

c. Table 3 depicts how the certification scheme relates to established cryptologic professional development paths, utilizing ICD Number 652 (Reference (q)).

Table 3. Developmental Path by Proficiency Level

Developmental Path for _____				
Competencies	Course/Developmental Activities	Work Level	Proficiency Level	Assessment Strategy
List Competencies	List Activities	Identify Work Level	Identify Proficiency Level	Identify Assessment Strategy

d. Table 4 depicts the certification scheme associated with each certification.

Table 4: Policy Matrix

POLICY MATRIX FOR A CRYPTOLOGIC CERTIFICATION			
CERTIFICATION NAME			
INTENDED AUDIENCE	Cryptologic professionals performing: [List of Functional Tasks]		
CRYPTOLOGIC PROFESSIONAL NEEDS:	PREREQUISITES	REQUIREMENTS	WAIVERS
	• Applicable and approved prerequisites	• Approved assessment processes	• Approved waivers
CERTIFICATION RENEWAL			
CERTIFICATION MAINTENANCE REQUIREMENTS	Approved continuing education units per year, when applicable.		
RECERTIFICATION REQUIREMENTS	Conditions or events that trigger the need for recertification and assessment processes used for recertification.		

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ADET	Associate Director for Education and Training
ADHR	Associate Director for Human Resources
CTC	Cryptologic Training Council
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoDD	DoD Directive
DoDI	DoD Instruction
IC	Intelligence Community
ICD	Intelligence Community Directive
NCCA	National Commission for Certifying Agencies
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
ODNI	Office of the Director of National Intelligence
PDD	program design document
PPBE	Planning, Programming, Budgeting, and Execution
SAV	staff assistance visit
SHCP	strategic human capital planning
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this manual.

accomplishment record. Written descriptions of past achievements related to required qualification standards.

accreditation. Defined in Reference (b).

assessment strategies. Specific certification requirements related to specified categories of persons to which the same particular standards, rules, and procedures apply.

candidate. An individual who has met the eligibility qualification for but has not yet earned a credential awarded through a certification program.

certification. Defined in Reference (b).

certification blueprint. A document that specifies segments of the cryptologic essential body of knowledge a particular certification covers. It describes the knowledge and skills individuals must demonstrate to obtain the certification, and it informs others about the specific set of knowledge and skills certification holders possess as a function of holding that certification.

certification framework. A representation of a certification program's offerings that reflects the sequence with which individuals are expected to acquire the knowledge and skills specified in the cryptologic essential body of knowledge. It presents a notional career pathway that uses certifications as career benchmarks or milestones. It also defines an individual's progression through a certification program.

certification renewal. An effort to measure continuing competence of cryptologic personnel.

certification scheme. Standardized set of assessment processes to uniformly evaluate individuals' mastery of a predefined segment of the cryptologic essential body of knowledge associated with a particular certification. It specifies eligibility, assessment strategies, and renewal requirements.

competencies. Defined in Reference (i).

competency directory. Defined in Reference (i).

cryptologic certification program. The umbrella term for all cryptologic certifications outlined in this manual.

cryptologic essential body of knowledge. The cryptologic community's job analysis results are documented specifying the community's functional tasks and the knowledge and skills required to perform those functional tasks. It documents how those knowledge and skills are aligned with relevant ODNI competency directories. It describes the community's expectation of what individuals need to know and be able to do to be a high-performing contributor and member of the community.

externally accredited certification program. External recognition is required when a certification program applies to more than one component workforce segment preparing such personnel for duty with other departments, agencies, and elements of the IC pursuant to Reference (l).

functional tasks. A set of mutually exclusive segments or concentrations of work that are performed to fulfill organizational goals and objectives. Also referred to as "capabilities" in the skill standards development process.

high stakes decisions. Decisions linking certification assessments results used to support personnel decisions and the process of selection of personnel for a work role, function, or position; placement of personnel into work role, function, or position; or continued service or employability of personnel in a work role, function, or position.

incumbent. An incumbent is a cryptologic employee encumbering a function, position, or work role that has been coded as requiring the certification, but who was hired for that function, position, or work role prior to its being designated as requiring a certification. As the cryptologic certification was not a condition of employment at the time of hire, the employee is not required to become certified to remain in that function, position, or work role. However, should that employee desire or accept any other coded function, position, or work role (including lateral moves and promotions) that identifies a requirement for certification, the employee is required to fulfill the conditions of employment for the new function, position, or work role within the timeframe required, as specified by the employing agency.

institutional accreditation. Education and training organizations supporting cryptologic certification programs are required to seek institutional accreditation, which must be achieved by meeting the published standards and the associated criteria of a U.S. Secretary of Education-recognized accrediting agency, such as the Council on Occupational Education.

NSA Cryptologic Certification Program. A high rigor certification program requiring individuals to complete a consistent set of development activities and successfully pass one or more standardized assessments. The NSA Cryptologic Certification Program is for a homogeneous workforce segment.

PDD. Codifies policies and procedures of a certification program. It provides stakeholders visibility into the strategic, operational, and technical elements of a certification program. Documentation required for accreditation of the certification program is included.

performance evaluation. Required performance appraisal ratings and specific accomplishments other assessment strategies do not capture.

proficiency. Defined in Reference (q).

psychometrics. The field of study concerned with the theory and technique of educational and psychological measurement, which includes the measurement of knowledge, abilities, attitudes, and personality traits. The field is primarily concerned with the study of measurement instruments such as questionnaires and tests.

standardized assessments. Structured strategy used to measure capabilities and competencies.

work levels. Defined in Reference (q).

work products. Deliverables or outcomes the individual must produce to provide evidence the candidate has attained a level of capability.