

NCMS, INC.

The Society of Industrial Security Professionals



Industrial Security Professional (ISP)

Certification Program Requirements and Application

last update: April 2010

Developed & administered by the
NCMS, Inc.

994 Old Eagle School Road, Suite 1019
Wayne, PA 19087

(610) 971-4856 Fax: (610) 971-4859

Email: info@classmgmt.com Web Site: www.classmgmt.com

Table of Contents....

Message from the NCMS President.....	page 2
ISP Code of Ethics.....	page 2
The Certification Exam.....	page 3
Certification Criteria.....	page 3
The Test.....	page 3
References.....	page 4
Recertification.....	page 4

The NCMS Industrial Security Professional (ISP) Certification Program

From the NCMS President...

The NCMS is proud to announce the Industrial Security Professional (ISP) Certification Program. Led by James Hickok, PhD, Chairperson of the Education & Training Committee, the Society is providing a new professional certification to qualified candidates who work within the U.S. National Industrial Security Program (NISP).

The intent of the ISP designation is to award professional certification and recognition to qualified candidates who demonstrate the knowledge, skills, and abilities their profession demands. The basis for the examination is primarily the National Industrial Security Program Operating Manual (NISPOM), the supplements, and other information security concomitant rules and regulations to include Operations Security, proprietary information, etc.

Successfully completing the examination will signify the overall competence of the candidate on NISPOM requirements, so current and prospective employers will have a recognized criteria to evaluate their performance.

The NCMS Professional Certification Program is the result of a three year effort by the Society's Education & Training Committee, as well as the Chapter Chairpersons and the National Board of Directors.

PURPOSE:

The purpose of the ISP certification is two-fold:

- 1) to provide recognition of the professional training and qualifications of veterans of industrial and government security, and
- 2) to provide guidelines for professional training needed by new security employees.

WHY DEVELOP OUR OWN PROGRAM?

NCMS developed its own certification program because the Society saw a need to focus specifically on the needs of the Industrial Security Professional and to provide a vehicle for recognition of individuals who have achieved a standard of excellence in the field of industrial security.

WHAT DO WE HOPE TO ACCOMPLISH?

- Increase the professionalism within industry and government security;
- Enhance the recognition of industry and government security professionals;
- Increase the recognition of the NCMS as a premier security organization;

- Improve the cooperation between government and industry security personnel;
- Improve the security of national-security-related assets.

If you have any questions about the program, please visit our website at www.isp.org.

ISP CODE OF ETHICS

ISPs and ISP candidates must always demonstrate the highest levels of professional behavior and integrity, which includes, but is not limited to, the characteristics listed below.

- Act in an honest, forthright, and dependable manner.
- Follow and enforce all applicable security laws, regulations, orders, rules, policies, and procedures.
- Safeguard classified and proprietary information at all times.
- Place national security above all other work priorities.
- Maintain proficiency in the appropriate security fields.
- Assist fellow security professionals who are in need.
- Balance security needs with operational and research requirements.
- Refrain from negative actions such as starting rumors, making slanderous statements, and embarking on character assassination.

DISCIPLINARY ACTIONS. Any NCMS member or ISP should submit in writing any instances of unprofessional or unethical behavior to the NCMS Executive Director. All disciplinary issues will be reviewed by the NCMS Board of Directors, who will determine what, if any, disciplinary actions are appropriate.

REASONS FOR DISCIPLINARY ACTIONS. The reasons for disciplinary actions include, but are not restricted to, the following actions:

- Conviction on felony charges.
- Failure to abide by the ISP Code of Ethics.

THE CERTIFICATION EXAM

Administration of the Exam

1. The main test has 100 questions.
2. Candidate also selects from two of the four elective topics for 10 additional questions.
3. Candidate will have two hours to complete the test.
4. The test will be proctored with an NCMS-approved instructor in one of two ways:
 - a. via hard copy test and answer sheet (only at the Annual Training Seminar) **OR**
 - b. on-line, using Thomson-Prometric, Inc. testing services.

**Note: The application process and requirements are the same whether candidate is taking a hard copy or an on-line test.*

5. Proctor Qualifications
 - a. ISP. This is the preferred qualification; all others will be by exception.
 - b. Other Proctor Types:
 - i. Official Proctor (company or individual)
 - ii. Teacher/Trainer/Professor
 - iii. Security Professional
 - iv. Government Official
 - c. In all cases, the qualifications must be verified in writing and sent in with the candidate's ISP application for approval prior to administering the examination.
 - d. There are no specific qualifications for each category of potential proctor; the "reasonable person" theory will be used when determining the qualifications of the proctor. The ISP committee is looking for reliable professionals as a general rule.
 - e. Any non-ISP proctor must be a disinterested third party, i.e., they must be totally dispassionate about the results of the examination. For example, a candidate's boss, relative, good friend, co-worker, or significant other would not be considered a disinterested third party.
 - f. If a non-ISP security professional proctors the examination, he or she is ineligible to take the ISP examination at any time thereafter.
6. The test is "open book". A complete list of reference sources is available at <http://www.ncms-isp.org>. Candidates may use these sources during the test. The duration of the test, however, does not allow for extensive use of these sources to answer the questions. Candidates may not reach out to other people during the test, whether in person or by phone, text messages, email, instant messaging, or by any other means.

7. If a candidate fails the test:
 - a. the test may be retaken after a waiting period of six months, and payment of a \$75 processing fee is required;
 - b. a new application and collateral materials are not required if current data has not changed and candidate is taking the test within one year of approval of the original application;
 - c. if any data has changed (i.e. new supervisor, new employment), candidate is required to submit updated materials;
 - d. if original application is more than 12 months old when candidate provides written notice of intent, then a new application and collateral materials is required.
8. If a candidate fails the test a second time, a new application and collateral materials will be required after a six month waiting period, and the entire fee must be paid.

CERTIFICATION CRITERIA

Training

- Pass the ISP exam with a score of at least 75% correct; **OR**
- DOE candidates may substitute for the ISP exam the successful completion of the DOE Professional Enhancement Program in at least one security track from INFOSEC; PERSEC; PHYSEC; or Program, Planning, and Management.

Experience

- At least five years experience in industrial security.
- Candidates must be working in security at least part-time as part of their job description (a minimum of 10% of hours worked).

Recommendation

- A written recommendation is required from a supervisor. If the candidate does not have a supervisor, he or she should contact their chapter chair for further guidance.

Application/Payment

- A completed application, along with payment in full, must be received **at least 30 days prior** to the scheduled test date, whether the test will be hard-copy format or on-line. *Note: you must have arranged for a proctor, along with a time/date for the test before submitting your application. This information is to be included on the application.*

- Candidates taking the test on-line will receive test taking instructions from the National Office upon approval of application and will need to register as a user with Thomson-Prometric prior to taking the test. The proctor will receive the eligibility code that will be used for taking the test along with a packet of proctoring materials.

THE TEST

Required and Elective Categories

For DOD security professionals, the skills required for certification will fall into the following areas:

1. Security Administration & Management
 - a. Records, Planning & Budgeting
 - c. Staffing
 - d. Facility Clearances & Approvals
 - e. Special forms (254, 441, etc.)
 - f. Escorting Uncleared US Nationals
 - g. Incidents of Security Concern
 - h. Risk Management
2. Document Security
 - a. Creation & Marking
 - b. Storage & Accountability
 - c. Transmission & Receiving
 - d. Reproduction & Destruction
 - e. End of Contract Actions
 - f. Emergency Actions and Physical Protections
 - h. Access Controls
3. Information Systems Security
 - a. System Security Plans
 - b. Accreditation
 - c. Physical Protections
 - d. Administrative & Procedural Controls
 - e. Forensics
 - f. Reporting & Records
 - g. Destruction
4. Physical Security
 - a. Theory: Graded & Layered Protection
 - b. Locks & Security Containers
 - c. Vaults & Vault-type Rooms
 - d. Alarms
 - e. CCTV
 - f. Central Alarm Stations & Requirements
 - g. Access Controls and Guards
 - i. Records
5. Personnel Security
 - a. Forms
 - b. Adjudication
 - c. EPSQ/JPAS
 - d. Clearances & Badges
6. International Security
 - a. Export Control Regulations
 - b. Foreign Visits & Assignments
 - c. Foreign Ownership, Control or Influence
 - d. Controlling Access by Foreign Persons

7. Classification
 - a. Identifying Critical Information
 - b. Classification System & Guides
 - d. Declassification
 - e. Records
8. Security Education
 - a. Requirements and Content
 - c. Ideas & Techniques
9. Audits & Self-Assessments
 - a. Audits
 - b. Self-Assessments
10. Electives
 - a. Intellectual Property
 - b. COMSEC/TEMPEST
 - c. Counterintelligence
 - d. Operations Security (OPSEC)

References

**For a complete listing of suggested references, please go to the web site at www.ncms-isp.org*

RECERTIFICATION

- Candidates must recertify every three years by the last day of the month in which the candidate originally became certified.
- Six (6) recertification credits are required for certification.
- All requests for credits to be used for recertification will be adjudicated by NCMS.
- Some or all of your activities may qualify for credit under more than one professional certification.
- No more than 50% of the claimed recertification credits can come from Membership and Voluntary Service activities. At least 50% of the credits must come from Educational Programs and Courses, Instruction, Speeches, and Other Presentations, or Publications.
- The same activity may not be counted under more than one category. (For example, a presentation originally given orally cannot be published and counted both as a presentation and as a published article.)
- Documentation to support claimed recertification credits is required.

For complete information on recertification, please go to the web site at www.ncms-isp.org.