Table of Contents....

Program Overview .................................................................................... page 2
ISP® Code of Ethics .................................................................................. page 2
The Certification Exam ............................................................................. page 3
Certification Criteria .................................................................................. page 3
The Test .................................................................................................... page 4
References ............................................................................................... page 4
Recertification .......................................................................................... page 4
NCMS is proud to offer the Industrial Security Professional (ISP®) Certification Program. Originally led by James Hickok, PhD, Past President of the Society, in coordination with the NCMS Board of Directors and Chapter Chairs, the Society has provided this professional certification to qualified candidates who work within the U.S. National Industrial Security Program (NISP) since 2004.

The intent of the ISP® program 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 signifies the overall competence of the candidate on NISPOM requirements, so current and prospective employers will have a recognized criteria to evaluate their performance.

**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.

**IMPARTIALITY:**
NCMS is dedicated to ensuring that the ISP® Certification Program is organized and administered in an impartial and fair manner; thereby avoiding conflicts of interest and outside influence, while ensuring an impartial and fair program.

**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.ncms-isp.org.

**ISP® CODE OF ETHICS**
ISP®s and ISP® candidates must always demonstrate the highest levels of professional and ethical behavior, with unquestionable 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.
- Making false official statements or claims.
THE CERTIFICATION EXAM

Administration of the Exam
1. The main test has 100 questions.
2. Candidate also selects from two of the five elective topics for a total of 10 additional questions.
3. Candidate will have two hours to complete the test.
4. All tests will be proctored with an NCMS-approved proctor.
5. The exam fee is $275/NCMS Members; $400/non-members. There is a $50 surcharge for international candidates.

6. Proctor Qualifications
   a. ISP®. This is the preferred qualification; all others will be approved by the committee.
   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 proctor must provide a written affidavit certifying he/she meets the qualifications, which will be included with the candidate’s ISP® application package for approval by the committee.
   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.
   e. Any proctor must be a “disinterested third party”, someone who is 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.

7. The test is open book. A list of reference sources is available at http://www.ncms-isp.org. Candidates may use these sources during the exam, but internet access, except to access the exam, is not permitted at any time. Candidates may bring their reference materials to the exam either in hard copy or on a separate laptop.

8. If a candidate fails the test:
   a. the test may be retaken after six months;
   b. candidate must apply online to retest at least 30 days in advance of the proposed test date, with date/location of the exam and proctor information;
   c. a retest fee of $140 (NCMS members) or $200 (non-members) must accompany the letter;
   d. 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;
   e. if any data has changed (i.e. new supervisor, new employment), candidate is required to submit updated materials;
   f. if original application is more than one year old, then a new application and collateral materials are required.

9. 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.

10. Special Needs Candidates
    Candidates may request special consideration or accommodation in writing to the Executive Director, who will forward the request to the ISP® Committee Chair for resolution. All requests must include the specific condition that requires the accommodation and a doctor’s written verification of the condition creating the need for accommodation.

CERTIFICATION REQUIREMENTS

Experience
- At least five years cumulative 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) in order for the experience to qualify.
- Candidates do not need to be currently working in industrial security to apply for the exam as long as their work history satisfies the five year requirement.

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

Proctor Information
- A signed affidavit from your proctor is required (see #6 in previous section), proctor contact information, and a date, time, and location of the exam.

Application/Payment
- A completed application, along with payment in full, must be received at least 30 days prior to the scheduled test date.
- Candidates will receive instructions for taking the exam from the National Office upon approval of application and will need to register as a user with Prometric prior to taking the test. The proctor will receive the eligibility code that will be used for taking the test along with a proctor form and instructions.

Exam Performance
- Pass the ISP® exam with a score of at least 75% correct.
### RECERTIFICATION

- Candidates must recertify every three years by the last day of the month in which the candidate originally became certified.
- Sixty (60) CEUs are required for certification.
- All requests for CEUs to be used for recertification will be adjudicated by NCMS.
- The cost to recertify is $75/NCMS members; $125/non-members.
- No more than 50% of the claimed recertification CEUs can come from Membership and Voluntary Service activities. At least 50% of the CEUs must come from Security-related Educational Programs and Courses, Instruction, Speeches, and Other Presentations, or Publications.
- The same activity may not be counted under more than one category. (e.g., a presentation originally given orally cannot be published and counted both as a presentation and as a published article.)
- Documentation to support CEUs is required.

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

### 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**
   - Records, Planning & Budgeting
   - Staffing
   - Facility Clearances & Approvals
   - Special forms (254, 441, etc.)
   - Escorting Uncleared US Nationals
   - Incidents of Security Concern
   - Risk Management

2. **Document Security**
   - Creation & Marking
   - Storage & Accountability
   - Transmission & Receipting
   - Reproduction & Destruction
   - End of Contract Actions
   - Emergency Actions and Physical Protections
   - Access Controls

3. **Information Systems Security**
   - System Security Plans
   - Accreditation
   - Physical Protections
   - Administrative & Procedural Controls
   - Forensics
   - Reporting & Records
   - Destruction

4. **Physical Security**
   - Theory: Graded & Layered Protection
   - Locks & Security Containers
   - Vaults & Vault-type Rooms
   - Alarms
   - CCTV
   - Central Alarm Stations & Requirements
   - Access Controls and Guards
   - Records

5. **Personnel Security**
   - Forms
   - Adjudication
   - EPSQ/JPAS
   - Clearances & Badges

6. **International Security**
   - Export Control Regulations
   - Foreign Visits & Assignments
   - Foreign Ownership, Control or Influence
   - Controlling Access by Foreign Persons

7. **Classification**
   - Identifying Critical Information
   - Classification System & Guides
   - Declassification
   - Records

8. **Security Education**
   - Requirements and Content
   - Ideas & Techniques

9. **Audits & Self-Assessments**
   - Audits
   - Self-Assessments

10. **Electives**
    - Intellectual Property
    - COMSEC/TEMPEST
    - Counterintelligence
    - Operations Security (OPSEC)
    - SAP

---

### Required and Elective Categories

#### The Test

**1. Security Administration & Management**
   - Records, Planning & Budgeting
   - Staffing
   - Facility Clearances & Approvals
   - Special forms (254, 441, etc.)
   - Escorting Uncleared US Nationals
   - Incidents of Security Concern
   - Risk Management

**2. Document Security**
   - Creation & Marking
   - Storage & Accountability
   - Transmission & Receipting
   - Reproduction & Destruction
   - End of Contract Actions
   - Emergency Actions and Physical Protections
   - Access Controls

**3. Information Systems Security**
   - System Security Plans
   - Accreditation
   - Physical Protections
   - Administrative & Procedural Controls
   - Forensics
   - Reporting & Records
   - Destruction

**4. Physical Security**
   - Theory: Graded & Layered Protection
   - Locks & Security Containers
   - Vaults & Vault-type Rooms
   - Alarms
   - CCTV
   - Central Alarm Stations & Requirements
   - Access Controls and Guards
   - Records

**5. Personnel Security**
   - Forms
   - Adjudication
   - EPSQ/JPAS
   - Clearances & Badges

**6. International Security**
   - Export Control Regulations
   - Foreign Visits & Assignments
   - Foreign Ownership, Control or Influence
   - Controlling Access by Foreign Persons