THE SOCIETY OF INDUSTRIAL SECURITY PROFESSIONALS

Industrial Security Professional (ISP®) Certification Program Requirements and Application

Table of Contents

Document Number:
ISP - 3034

Version:
1.10

Revision Date:
April 2025

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: https://ncms-isp.org

INTRODUCTION

"The intent of the ISP® designation is to award professional certification and recognition to qualified candidates"

NCMS is proud to offer the Industrial Security Professional (ISP®) Certification. The Society is providing the 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, including 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

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 ARE OUR PROGRAM GOALS?

- Increase the professionalism within industry and government security;
- Enhance the recognition of industry and government security professionals;
- Increase the recognition of NCMS as a premier security organization;
- Improve the cooperation between government and industry security personnel;
- Improve the security of national security-related assets.

Questions? Please visit our website at https://ncms-isp.org.

EXAM ADMINISTRATION

1. The examination consists of 110 questions from **11** categories. (see "Required Categories".)

2. Candidate will have two and a half hours to complete the exam.

3. A score of 70% or greater is needed to pass.

4. All exams are conducted at Prometric test centers throughout the country and remote testing. Exam sessions will be scheduled through Prometric's online portal. Appointments are scheduled based on availability at each test center. Requested dates are not guaranteed.

5. To locate test centers near you, visit Prometric at: http://securereg3.prometric.com/landing.aspx?prg=NCMS&path=schd

6. The exam is "open book". The comprehensive list of exam references for the purpose of exam preparation is available at https://ncms-isp.org, and will be available during the exam.

7. If a candidate fails the exam:
- The exam may be retaken after 30 days;
- Candidate must apply online to retake the exam at least 30 days in advance of the anticipated exam date;
- A retake fee of $140 (NCMS Members) or $200 (non-members) must accompany the application;
- Updated collateral materials are only required if current data has changed and/or candidate is retaking the exam more than one year following approval of the original application;

8. Special Accommodations:
- Candidates may request special consideration or accommodation in writing to the Executive Director, for review and determination by the ISP® Committee;
- All requests must include the specific condition(s) that requires the accommodation and a doctor's written confirmation of the condition and reason for the request.

9. When a candidate passes the exam:
- Official written notification and ISP® pin will be sent from NCMS HQ within 10-15 business days;
- Certificate will follow within 4-6 weeks;
- Individual may begin using the ISP® designation immediately in accordance with the NCMS Appropriate Use policy (refer to the P&P Manual);
- It is the individual's responsibility to comply with all policies of the ISP® program.

CANDIDATE REQUIREMENTS

Experience:
- At least two years cumulative experience in industrial security (note: military/police/guard experience may not qualify);
- 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 be considered;
- Candidates do not need to be currently working in industrial security to apply as long as their work history satisfies the five year requirement;
- A current resume is required. Be as specific as possible regarding security experience.

Confidentiality/Conflict of Interest Form (CCOI):
- A signed CCOI is required from the candidate with the application. The form is available for download on the program's website.
- Failure to complete this form will result in application being denied.

Application/Payment:
- A completed application, along with payment in full, must be received at least 30 days prior to the anticipated exam date.
- Exam fees are $275 for NCMS Members; $400 for non-members.

Approval:
- Candidates will receive notification via email from NCMS HQ;
- If approved, candidates will have a six month eligibility window in which to take the exam;
- If a candidate fails to take the exam within this window, please contact the Executive Director to request an extension;
- If a candidate's application is not approved, the reason will be provided, and candidate will have the opportunity to reapply when all requirements are met.

Cancellation:
Prometric charges a cancellation fee if a session is cancelled less than 30 days prior to the scheduled exam date:

30+ days prior to exam date:	No Fee
5 – 29 days prior to exam date:	$50
Less than 5 days:	$70

NCMS charges a $50 fee for candidates who cancel after being approved to take the exam. These fees will be deducted from the original exam fee, and the candidate will be refunded the remaining funds. Cancellations must be first made directly with Prometric. The Executive Director must be notified in writing in order to receive any refunds.

Rescheduling:
Prometric charges reschedule fees if a session is rescheduled less than 30 days prior to the scheduled test date:

30+ days prior to exam date:	No Fee
5 – 29 days prior to exam date:	$50
Less than 5 days:	$70

NCMS does not charge a rescheduling fee. The candidate will not be permitted to reschedule until the fee is paid directly to Prometric. Rescheduling exam sessions must be made directly with Prometric.

Exam Questions Categories

Security Administration

- NISP General Requirements
- Reporting Requirements, inc. Cyber Incident Reporting
- Security Violations & Reporting
- Insider Threat Program
- Entity Eligibility Requirements & FCLs
- FOCI & SSA Issues
- Classified Meetings & Visits
- Subcontracting

Document Security

- Creating & Marking U.S. Classified Material
- Classified Working Papers
- Accountability
- Transmission, including Hand Carrying, & Receipting
- Destruction
- Reproduction
- Retention
- Information Management System Requirements

Information Systems Security

- IS Security Program Requirements
- ISSM, ISSO, & User Training & Responsibilities
- Risk Management Framework Process
- User Account & Password Requirements
- Marking IS Hardware & Media
- Auditing Requirements
- Assessment, Authorization, & Reauthorization
- Security Controls
- System Security Plans
- CSA Authorization
- Security Impact Levels

Physical Security

- General Safeguarding Requirements
- Security in Depth
- Storage Requirements
- Supplemental Controls
- Automated Access Control Systems
- Open Storage Area & Vault Construction & Requirements
- GSA Approved Container and Vault Door Repair
- IDS & Central Station Monitoring

Personnel Security

- E.O. 12968
- PCL Requirements
- Disqualifying Personal Issues
- SEAD 3 Reporting Requirements & Adverse Information
- SEAD 4 Adjudicative Guideline Requirements
- Temporary Eligibility Determinations & Limitations
- PCL Denial & Revocation
- Consultant & LAA Requirements
- Reciprocity Requirements

International Security

- Foreign Disclosure Criteria
- Bilateral Security Agreements
- Export Control Regulations
- Foreign Classified Contract Requirements
- FGI Classification Levels
- FGI Material Marking, Handling, & Storage Requirements
- Direct Commercial Sales Requirements
- International Transfers of Classified Material
- Foreign Visitors & International Meetings & Visits
- NATO Information Marking, Handling, & Storage Requirements
- International Subcontracting

Classification

- E.O. 13256 Requirements
- Original Classification
- Derivative Classification Requirements
- RD, FRD, & TFNI
- Downgrading & Declassification Procedures
- DD Forms 254 & Security Classification Guides
- Classification Challenges & Unsolicited Proposals
- Improperly Released Classified Information

Security Education

- FSO, Security Staff, ITPSO Training
- Initial & Refresher Security Briefings
- Security Debriefings
- SF 312 Issues
- Insider Threat Training

Audits & Self-Assessments

- Security Reviews/ Audits
- Self-Inspection Requirements
- SMO Security Responsibilities

Special Security Information

- Counterintelligence Issues
- COMSEC Basics
- Intellectual Property Issues, including FOIA and the Privacy Act, Trade Secrets, Copyrights, Patents, Trademark Basics
- OPSEC Basics

NISP Systems

- DISS
- NISS
- eApp
- eMASS

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 Ethics Committee, 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.

Note: Depending on current DCSA guidance, NBIS questions could be substituted for DISS questions. An announcement in advance of such a change will be published well before any change to the exam.