



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S10-001
IT Standard: Continuing Professional Education Requirements for Information Security Officers/Designated Security Representatives	Updated: 09/10/2018
	Issued By: NYS Office of Information Technology Services Owner: Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this standard is to outline the minimum requirements for continuing professional education (CPE) for members of the workforce who are serving in the role of Information Security Officer (ISO) or designated security representative for a State Entity (SE).

The requirement of CPE credits helps assure that these individuals stay current in this rapidly evolving field and maintain their breadth of knowledge.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

3.0 Scope

This standard applies to all “State Government” entities as defined in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law (“State Entities”), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. Where a conflict exists between this standard and a State Entity’s standard, the more restrictive standard will take precedence.

This standard applies to members of the State workforce who have been designated as the ISO or designated security representatives for an SE. This includes those within an information security business unit who fulfill the functional responsibilities of the ISO as outlined in the [Information Security Policy](#) and is not intended to include support staff.

4.0 Information Statement

Due to the dynamic nature of information technology and the need to maintain an adequate level of current knowledge and proficiency in information security, a minimum of thirty-seven and one half (37.5) hours of Continuing Professional Education (CPE) credits must be completed annually. The CPEs must be directly related to information systems security. The SE will provide the opportunity for the ISO/designated security representative to earn the required CPEs annually.

Criteria for qualifying the activities for CPE credits will be based on ISACA and ISC2 guidelines. In cases where there is a discrepancy between these guidelines, the lesser requirements apply.

The annual time period to earn CPE credits will coincide with the calendar year (January 1 to December 31). An individual’s cycle will begin the January following appointment to the ISO/designated security representative position. Credits must be earned during the current year to qualify and may not be carried forward or backward from year to year.

Approved information systems security categories include but are not limited to:

- Access control
- Telecommunications and network security
- Information security governance and risk management practices
- Software development security
- Cryptography
- Security architecture and design
- Operations security

- Business continuity and disaster recovery
- Law, regulations, compliance and investigation
- Physical (environmental) security

CPE credits are given for related experience outside of normal on-the-job duties. For instance, while time spent independently preparing an information security presentation for a community organization would qualify for CPE credits, an equivalent amount of time spent on the job preparing a staff presentation, other internal publications or events would NOT qualify.

CPE credits are weighted by activity. Below are common categories of activities and the amount of credits earned for each. These activities are not intended to be a complete listing, as many other events such as graduate work in an appropriate academic field, may also qualify. Typically you will earn 1 CPE credit for each hour spent engaged in an educational activity. However, some activities are worth more CPEs, due to the depth of study or ongoing commitment involved. CPE activities include but are not limited to:

- Earn 1 CPE credit for each hour of attendance at a security educational training course or seminar.
- Earn 1 CPE credit for each hour of attendance at a security conference. The New York State Cyber Security Conference qualifies for CPE credits.
- Earn 1 CPE credit for each hour of attendance at a State information security community of practice meeting or NYS Forum information security workgroup meeting.
- Earn 1 CPE credit for each hour of attendance at a professional security association chapter meeting, such as the International Information Systems Security Certification Consortium (ISC2), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), etc.
- Earn 1 CPE credit for each hour of attendance at a higher education academic security class. Credit will only be given on passing the course successfully.
- Earn CPE credits for preparing courseware, lectures, or training material. The time spent preparing for and delivering each hour of presentation material is valued at 4 CPE credits (e.g., a one hour presentation = 4 CPE's, a two hour presentation = 8 CPE's). The 4 CPEs for each hour of presentation will only be granted for the initial course, lecture or training presentation, thereafter you will receive 1 CPE for each hour of presentation.
- Earn CPE credits for contributing original work to the information systems security profession. First publication of a security related article will earn the author(s) 10 CPE credits. Publication of a security related book will earn 40 CPE credits.
- Earn up to 12 CPE credits per year, 1 for each month of service on the board of professional security organization, such as ISC2, ISSA, ISACA, etc.

- Earn 1 CPE for each month of active participation on a State or national information security workgroup or committee.
- Earn 1 CPE credit for each hour of attendance at security webcasts.
- Credits can be earned by completing a self-study program or completing computer-based training and the course provider issues a certificate of completion and supplies the number of CPE hours earned for the course. Study material and validated documentation of completion, such as a certificate or diploma, must be retained.
- Reading an information security text will be worth 2 CPE credits. Credit in this category will be limited to one text per year. If audited, the individual should retain proof of possession, such as the actual book, a sales receipt, invoice, library record, etc.
- Completion and submission of an original information security book review will be worth 3 CPE credits (limited to one text per year).
- Earn 1 CPE for each hour of attendance at a vendor security product training class or an information security specific sales presentation. Credits for a security sales presentation will be limited to 3 per year.
-

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S10-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
02/12/2010	Original Standard Release	
05/16/2014	Rebranded for the Office of Information Technology Services (<i>replaces CSCIC/OCS-S10-001 Role and Responsibilities of the State Entity Information Security Officer</i>); increase annual CPE requirements from 22.5 to 37.5 hours; allow CPE credits for NYS Forum security workgroup participation	Deborah Snyder, Deputy Chief Information Security Officer
05/15/2015	Added criteria for qualifying the activities for CPE credits based on ISACA and ISC2 guidelines	Deborah Snyder, Deputy Chief Information Security Officer
02/15/2017	Update of contact information and rebranding	Deborah Snyder, Deputy Chief Information Security Officer
09/10/2018	Scheduled review – no changes	Deborah A. Snyder, Chief Information Security Officer

9.0 Related Documents

[Information Systems Audit and Control Association \(ISACA\) Certified Information Systems Manager Continuing Professional Education Policy](#)

[ISC2 Continuing Professional Education Policies and Guidelines](#)