Comments of the
INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS
in response to the
NIST CYBERSECURITY WORKFORCE REQUEST FOR INFORMATION
JULY 28, 2017

I. Introduction

Knowledge of privacy laws and the ability to perform numerous privacy-related tasks are key features of the NICE Cybersecurity Workforce Framework. Information security systems are in place principally to protect against threats to personal information, enhancing the importance of privacy knowledge and skills among cybersecurity professionals.

These comments in response to the Cybersecurity Workforce RFI address the role of the International Association of Privacy Professionals (IAPP) in training and certifying privacy professionals as part of the cybersecurity workforce. The IAPP is a not-for-profit membership association organized under section 501(c)(6) of the U.S. Internal Revenue Code. The IAPP is a resource for professionals dedicated to helping their employers manage risks of data breach and lost consumer trust. With more than 30,000 members globally, the IAPP is the world's largest and most comprehensive privacy community.

To fulfill its mission -- to define, support and improve the privacy profession globally – the IAPP offers privacy training, professional certification, live events, web conferences, and daily news, research and information to help privacy professionals understand and keep abreast of the changing regulatory and risk landscape. The IAPP also supplies and helps privacy professionals find the resources they need to do their jobs, such as employee awareness training in privacy and security (our Privacy Core® programs); privacy impact assessments and data inventory tools; developing and maintaining programs for managing privacy and security risks throughout the enterprise; writing and updating internal policies for privacy, security, and incident response; guides for complying with the European Union's General Data Protection Regulation; preparing consumer-facing privacy statements; and the like.

II. General Information

A. Professional training and employee awareness training

The IAPP offers training for working professionals interested in gaining skills in privacy laws and regulations, technology related to information privacy protection, and privacy program management. Training options for those pursuing professional-level knowledge include two-day in-person live training with a skilled privacy practitioner, and online training (covering the same content as the two-day live training) for those who need to go at their own pace.

The IAPP also supports privacy professionals who have responsibility for developing and maintaining ongoing employee privacy and security awareness. One option is the IAPP's Privacy Core® program which can be used to help employees understand:

- why privacy matters;
- what personal information is and how to properly handle it;
- the role of security in protecting personal information;
- how to avoid phishing attacks and social engineering scams;
- how to build privacy by design into new products and services;
- the essentials of the GDPR;
- how to develop a sound vendor management program to protect personal information through contracts and audits; and
- other specialty privacy and security areas such as call center privacy issues, proper handling of children's information, employee monitoring, internet based advertising, and so on.

The training courses are helpful preparation for taking the IAPP's certification exams. For the United States cybersecurity workforce, the IAPP offers four certification options: Certified Information Privacy Professional for the U.S. private sector (CIPP/US); Certified Information Privacy Professional for the U.S. Government (CIPP/G); Certified Information Privacy Manager (CIPM); and Certified Information Privacy Technologist (CIPT).

B. Bodies of knowledge covered by IAPP training

1. CIPP/US Body of Knowledge

The basic information covered by the CIPP/US training is:

- Introduction to the U.S. Privacy Environment
- Limits on Private-sector Collection and Use of Data
- Government and Court Access to Private-sector Information
- Workplace Privacy
- State Privacy Laws

The body of knowledge covered by the CIPP/US exam can be found here: https://iapp.org/media/pdf/certification/CIPP_US_BoK_after%208.1.17.pdf .

2. CIPP/G Body of Knowledge

The basic information covered by the CIPP/G training is:

- U.S. Government Privacy Laws
- The Value of Privacy to U.S. Government Agencies

- U.S. Government Privacy Practices
- Privacy Program Management and Organization
- Privacy and the Federal Government Intelligence Community

The CIPP/G Body of Knowledge can be found here:
https://iapp.org/media/pdf/certification/CIPP_G_BoK.pdf

3. CIPM Body of Knowledge

The basic information covered by the CIPM training is:

- How to create a company vision
- How to structure the privacy team
- How to develop and implement a privacy program framework
- How to communicate to stakeholders
- How to measure performance
- The privacy program operational lifecycle

The body of knowledge for those exams, covered by the trainings, can be found here:
https://iapp.org/media/pdf/certification/CIPM_BoK.pdf

4. CIPT Body of Knowledge

The basic information covered by the CIPT training is:

- Critical privacy concepts and practices that impact IT
- Consumer privacy expectations and responsibility
- How to bake privacy into early stages of IT products and services for cost control, accuracy and speed-to-market
- How to establish privacy practices for data collection and transfer
- How to preempt privacy issues in the Internet of Things
- How to factor privacy into data classification and emerging tech such as cloud computing, facial recognition and surveillance
- How to communicate privacy issues with partners such as management, development, marketing and legal.

The body of knowledge covered by the CIPT training is:
https://iapp.org/certify/get-certified/cipt/

C. Relevance to the NICE Draft Cybersecurity Workforce Framework

The IAPP's training maps to over 70 elements of the draft NICE Cybersecurity Workforce Framework, as supplemented by the "Supplement to the NICE Specialty Areas and Work Role

KSAs and Tasks" issued in June 2017. Those elements are listed in the Appendix to these Comments.

III. Growing and Sustaining the Nation's Cybersecurity Workforce

The following comments seek to address selected questions raised in the RFI.

A. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce?

Government contracts now require that contractors implement and maintain rigorous cybersecurity training programs for employees. One way NIST can support heightened skills, training, and awareness of privacy as a component of cybersecurity – clearly one significant enough to merit over 70 KSAs and tasks in the forthcoming Cybersecurity Workforce Framework – is to **integrate privacy training requirements into standard procurement contracts**. This will enhance and support other basic security awareness training and reduce the threat of security breaches by increasing staff and employee sensitivity to the proper collection and use of personal information.

B. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today and what makes them effective?

Privacy – and other components of managing information and information systems – is a field that requires knowledge, skills and awareness in multiple disciplines, including technology, law, management, public policy, ethics, and business. Programs are being developed at the graduate and professional levels, at universities across the United States, that aim to bring these domains together if not in a degree program at least in some of the offered courses. These programs should be modeled, studied for best practices, described in research, and ultimately promoted through workshops, scholarships and grants that help the workforce develop skills across disciplines to better assess, manage and mitigate privacy and security risk.

Following are some examples of degree or certificate programs that are setting early standards for multi-disciplinary education.

Santa Clara Law School: Privacy Law Certificate Program
University of Maine School of Law: Certificate in Information Privacy Law
Carnegie Mellon University: Master of Science in Information Security and Management
Indiana University Maurer School of Law: Graduate certificate in information privacy law and policy
Boston College: Master of Science in Cybersecurity Policy and Governance
Brown University: Executive Master in Cybersecurity

Albany Law School: Master of Science in Legal Studies with a Concentration in Cybersecurity and Data Privacy

We encourage federal funding to support studying these programs to learn what works – and what doesn't – and to fund research, outreach, and ultimately curriculum development to establish successful multi-disciplinary graduate and professional degree programs nationwide.

C. How will advances in technology or other factors affect the cybersecurity workforce needed in the future?

In a global economy, information flows do not recognize borders. Customer data gathered by U.S. companies is not limited to U.S. citizens and is not always stored in the U.S. One of the future factors affecting the cybersecurity workforce is a need for greater understanding of global privacy and security standards, and a heightened awareness and knowledge of privacy by design. It is now well established –as reflected by the GDPR, Canada's Personal Information Protection and Electronic Documents Act, and the U.S. Federal Trade Commission's guidelines – that privacy should be baked into new technology products and services from their inception. The GDPR is a game-changing regulation that affects many U.S. companies' standard privacy and security practices. The cybersecurity workforce of *today* – not just the future – must be prepared to accommodate global privacy standards in their everyday tasks and responsibilities.

Appendix attached

APPENDIX

NICE Cybersecurity Workforce Framework KSAs and Tasks Addressed by the IAPP's Training

K0066: Knowledge of Privacy Impact Assessments.
K0168: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.
S0354: Skill in creating policies that reflect the business's core privacy objectives.
S0355: Skill in negotiating vendor agreements and evaluating vendor privacy practices.
A0110: Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.
A0111: Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
A0112: Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
A0113: Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
A0114: Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
A0115: Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
T0861: Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.
T0862: Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
T0863: Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
T0865: Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.
T0866: Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
T0867: Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
T0868: Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.
T0869: Work with organization senior management to establish an organization-wide Privacy Oversight Committee
T0870: Serve in a leadership role for Privacy Oversight Committee activities
T0871: Collaborate on cyber privacy and security policies and procedures

T0872: Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation
T0873: Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations
T0876: Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
T0877: Work cooperatively with applicable organization units in overseeing consumer information access rights
T0880: Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations
T0881: Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties
T0882: Conduct on-going privacy training and awareness activities
T0883: Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security
T0884: Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.
T0885: Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee
T0886: Work with External Affairs to respond to press and other inquiries with regard to concern over consumer and employee data
T0887: Provide leadership for the organization's privacy program
T0888: Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization
T0889: Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable
T0890: Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures
T0891: Resolve allegations of non-compliance with the corporate privacy policies or notice of information practices
T0892: Develop and coordinate a risk management and compliance framework for privacy
T0893: Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.
T0894: Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations
T0895: Establish a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization's privacy policies and procedures
T0896: Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity

T0897: Provide leadership in the planning, design and evaluation of privacy and security related projects
T0898: Establish an internal privacy audit program
T0899: Periodically revise the privacy program in light of changes in laws, regulatory or company policy
T0900: Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel
T0901: Assure that the use of technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information
T0902: Monitor systems development and operations for security and privacy compliance
T0903: Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected
T0904: Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions
T0905: Review all system-related information security plans to ensure alignment between security and privacy practices
T0906: Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements
T0907: Account for and administer individual requests for release or disclosure of personal and/or protected information
T0908: Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements
T0909: Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed
T0910: Act as, or work with, counsel relating to business partner contracts
T0911: Mitigate effects of a use or disclosure of personal information by employees or business partners
T0912: Develop and apply corrective action procedures
T0913: Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel
T0914: Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations
T0915: Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations
T0916: Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units
T0917: Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices
T0918: Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations

T0919: Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials

T0920: Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of non-compliance

T0921: Determine business partner requirements related to the organization's privacy program

T0922: Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company's privacy policies and procedures

T0923: Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations

T0924: Perform ongoing privacy compliance monitoring activities

T0925: Monitor advancements in information privacy technologies to ensure organization adoption and compliance

T0926: Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations