



STATE OF VERMONT
JOINT FISCAL OFFICE

MEMORANDUM

To: Joint Fiscal Committee Members
From: Nathan Lavery, Fiscal Analyst
Date: April 8, 2014
Subject: Grant/Position Request

Enclosed please find four (4) items that the Joint Fiscal Office has received from the administration. Seventeen (17) limited service positions are associated with these items.

JFO #2673 – \$52,000 grant from the Massachusetts Attorney General to the Vermont Office of the Attorney General. These funds will be used to offer a training program for data security certification. The Vermont Attorney General will host the International Association of Privacy Professionals training on behalf of a number of participating state Attorneys General. The training will include participants from Vermont. *[JFO received 03/25/14]*

JFO #2674 – In-kind donation of \$150,000 worth of services from Smart Growth America to the Vermont Agency of Transportation. Smart Growth America will provide technical assistance (in the form of facilitated outreach and training) for the development of an update to the Vermont State Design Standards. *[JFO received 3/25/14]*

JFO #2675 – \$150,000 grant from the U.S. Department of Energy to the Vermont Public Service Department. These funds will pass through the Clean Energy States Alliance, Inc., to the Public Service Department. The funding will be used to develop a plan for reducing “soft costs” associated with photovoltaic installations in Vermont, with a particular emphasis on the Burlington area. Soft costs are construction costs other than labor and materials, such as architectural, engineering, and legal costs. *[JFO received 03/25/14]*

JFO #2676 – Seventeen (17) limited service positions in the Agency of Human Services. These positions will assist in the process of bidding, evaluating, and selecting a new Medicaid Management Information System (MMIS) vendor. The positions are 90% federally funded (salary and benefits) and funding is included in the AHS annual budget. *[JFO received 03/28/14]*

Please review the enclosed materials and notify the Joint Fiscal Office (Nathan Lavery at (802) 828-1488; nlavery@leg.state.vt.us) if you have questions or would like an item held for legislative review. Unless we hear from you to the contrary by April 18 we will assume that you agree to consider as final the Governor’s acceptance of these requests.



State of Vermont
 Department of Finance & Management
 109 State Street, Pavilion Building
 Montpelier, VT 05620-0401

[phone] 802-828-2376
 [fax] 802-828-2428

Agency of Administration

JFO 2673

**STATE OF VERMONT
 FINANCE & MANAGEMENT GRANT REVIEW FORM**

Grant Summary: This grant will be used to pay for training and testing for a data security certification provided by the IAPP. Vermont will administer the Data Security funds to participating state AG offices, which will be sufficient to pay for 50 participants.

Date: 3/12/2014

Department: Office of the Attorney General, Public Protection Division

Legal Title of Grant: TJX Data Security Fund Grant

Federal Catalog #:

Grant/Donor Name and Address: Commonwealth of Massachusetts
 Data Security Fund Committee, Office of the Massachusetts Attorney General, Consumer Protection Division, 1 Ashburton Place, Boston, MA 02108

Grant Period: From: 3/1/2014 To: 12/31/2014

Grant/Donation \$52,000.00

	SFY 1	SFY 2	SFY 3	Total	Comments
Grant Amount:	\$52,000	\$	\$	\$52,000	

Position Information:	# Positions	Explanation/Comments
	0	

Additional Comments: .
 Has Vantage budget detail been reviewed and reconciled? Yes No HC (Analyst Initial)

Department of Finance & Management	RECEIVED MAR 20 2014 JOINT FISCAL OFFICE	SL 3/13/14 (Initial)
Secretary of Administration		MA 03/13/14 (Initial)
Sent To Joint Fiscal Office		3/21/14 Date

STATE OF VERMONT REQUEST FOR GRANT (*) ACCEPTANCE (Form AA-1)

BASIC GRANT INFORMATION				
1. Agency:				
2. Department:		Office of the Attorney General		
3. Program:		Public Protection Division		
4. Legal Title of Grant:		TJX Data Security Fund Grant		
5. Federal Catalog #:				
6. Grant/Donor Name and Address:				
Commonwealth of Massachusetts Data Security Fund Committee, Office of the Massachusetts Attorney General, Consumer Protection Division, One Ashburton Place Boston, MA 02108				
7. Grant Period:		From:	3/1/2014	To: 12/31/2014
8. Purpose of Grant:				
This grant will pay for training and testing for a data security certification (CIPP/US) provided by the International Association of Privacy Professionals ("IAPP"). Vermont is administering the funds, which will be issued by the Data Security Fund, and paid by Vermont to IAPP, on behalf of additional participating state AG Offices. The exact number of offices has not been determined yet, but the total amount to be distributed is \$52,000, enough to pay for 50 participants, of whom one or two will be from Vermont.				
9. Impact on existing program if grant is not Accepted:				
There will be no impact if the grant is not accepted.				
10. BUDGET INFORMATION				
	SFY 1	SFY 2	SFY 3	Comments
Expenditures:	FY 2014	FY 2015	FY	
Personal Services	\$	\$	\$	
Operating Expenses	\$	\$	\$	
Grants	\$52,000	\$	\$	
Total	\$	\$	\$	
Revenues:				
State Funds:	\$	\$	\$	
Cash	\$	\$	\$	
In-Kind	\$	\$	\$	
Federal Funds:	\$	\$	\$	
(Direct Costs)	\$	\$	\$	
(Statewide Indirect)	\$	\$	\$	
(Departmental Indirect)	\$	\$	\$	
Other Funds:	\$	\$	\$	
Grant (source TJX Data Security Fund) -	\$52,000	\$	\$	
Total	\$52,000	\$	\$	
Appropriation No:		2100001000 / Fund 21908	Amount:	\$52,000
			Total	\$52,000

STATE OF VERMONT REQUEST FOR GRANT (*) ACCEPTANCE (Form AA-1)

Has current fiscal year budget detail been entered into Vantage? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--

PERSONAL SERVICE INFORMATION

11. Will monies from this grant be used to fund one or more Personal Service Contracts? Yes No
 If "Yes", appointing authority must initial here to indicate intent to follow current competitive bidding process/policy.

Appointing Authority Name: _____ Agreed by: _____ (initial)

12. Limited Service Position Information:	# Positions	Title
Total Positions		

12a. Equipment and space for these positions: Is presently available. Can be obtained with available funds.

13. AUTHORIZATION AGENCY/DEPARTMENT

I/we certify that no funds beyond basic application preparation and filing costs have been expended or committed in anticipation of Joint Fiscal Committee approval of this grant, unless previous notification was made on Form AA-1PN (if applicable):	Signature:	Date: 3-5-14
	Title: William E. Griffin, Chief Assistant Attorney General	
	Signature: _____	Date: _____
	Title: _____	

14. SECRETARY OF ADMINISTRATION

<input checked="" type="checkbox"/>	Approved:	(Secretary or designee signature)	Date: 03/13/14
-------------------------------------	-----------	-----------------------------------	----------------

15. ACTION BY GOVERNOR

<input checked="" type="checkbox"/>	Check One Box: Accepted	(Governor's signature)	Date: 3/21/14
<input type="checkbox"/>	Rejected		

16. DOCUMENTATION REQUIRED

Required GRANT Documentation	
<input checked="" type="checkbox"/> Request Memo <input type="checkbox"/> Dept. project approval (if applicable) <input checked="" type="checkbox"/> Notice of Award <input type="checkbox"/> Grant Agreement <input checked="" type="checkbox"/> Grant Budget	<input type="checkbox"/> Notice of Donation (if any) <input type="checkbox"/> Grant (Project) Timeline (if applicable) <input type="checkbox"/> Request for Extension (if applicable) <input type="checkbox"/> Form AA-1PN attached (if applicable)

End Form AA-1

(*) The term "grant" refers to any grant, gift, loan, or any sum of money or thing of value to be accepted by any agency, department, commission, board, or other part of state government (see 32 V.S.A. §5).

**APPLICATION FOR DISTRIBUTION FROM
DATA SECURITY FUND**

I. APPLICANT

Name: Vermont Attorney General's Office
Address: 109 State St.
Montpelier, VT 05602

Contact Person(s) Ryan Kriger

Phone Number: 802-828-3170
Fax Number: 802-828-2154
E-mail: rkriger@atg.state.vt.us

Date of Application. November 8, 2013

II. STATUS OF APPLICANT

The Data Security Fund is for the exclusive use of the Offices of the Attorneys General of the Participating States.¹

A. Describe the applicant's function and responsibilities.

This application is being submitted by the Vermont Attorney General's Office ("VT AGO") on behalf of the AGO's of Vermont and several other states, including Arizona, Arkansas, Florida, Illinois, Iowa, Louisiana, Nebraska, Ohio, New Jersey, New York, and Texas (the "Applicant States").²

The Public Protection Division of the VT AGO enforces Vermont's data privacy laws and Consumer Fraud Act. Vermont's data privacy laws include the Security Breach Notice Act, 9 V.S.A. § 2435, and the Social Security Number Protection Act, 9 V.S.A. § 2440. Neither law affords a private right of action. When the Division becomes aware of a security breach affecting Vermont consumers, it reaches out to the affected business in order to ensure compliance with the law and to ensure that the vulnerability that permitted the breach is being remedied, and also posts the consumer notice letter required under the law on the Office website.

¹ The Participating States are: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia, Wisconsin, and the District of Columbia.

² Additional states may wish to join this group as described in Section G

The Division also conducts outreach to Vermont businesses, law enforcement, and the financial and technology communities. The goal of this outreach is to educate Vermonters and Vermont businesses about their legal obligations under Vermont's data privacy laws, to encourage businesses to enhance their data security, and to promote prompt and effective responses to data breaches occurring in Vermont.

The Division is also active in multistate investigations concerning privacy and security breaches.

B. Identify those persons who would oversee the proposed project.

Assistant Attorney General Ryan Kriger would be responsible for implementing the grant and Chief of the Public Protection Division Wendy Morgan would oversee the proposed project. NAAG would assist in overseeing the project.

III. APPLICANT'S PROPOSAL

A. Please state the anticipated public benefit to be served by the grant, including the target region and group, and how the benefit will be achieved.

The Public Protection Division of the VT AGO requests funding from the TJX Data Privacy Fund to fund training for at least 25 Assistant Attorneys General in the Applicant States, and support staff, to obtain training in data privacy laws, and to obtain certification from the International Association of Privacy Professionals ("IAPP"). The total amount of funding will depend on the number of participants in the program, but will likely range between \$26,250 and \$52,500. See Section G for a description of how this program would be implemented.

IAPP is a not for profit organization, founded in 2000, that serves as a resource for professionals working in the fields of privacy and data security³ It has over 13,000 members in 78 countries. Several AAG's working in privacy are currently members of the IAPP, which costs \$100/year for government employees.

IAPP offers a credential titled "Certified Information Privacy Professional/United States ("CIPP/US")⁴, which requires extensive knowledge of privacy and data security laws and contracts. Topics covered under the certification include:

- The U.S. legal system. definitions, sources of law and sectoral model for privacy enforcement
- U.S. federal laws for protection of personal data. FCRA and FACTA, HIPAA, GLBA, COPPA and DPPA

³ Further information about IAPP can be found at https://www.privacyassociation.org/about_iapp

⁴ Further information on this certification can be found at https://www.privacyassociation.org/certification/cipp_certification_programs.

- U.S. federal regulation of marketing practices: TSR, DNC, CAN-SPAM, TCPA and JFPA
- U.S. state data breach notification and select state laws
- Regulation of privacy in the U.S. workplace: FCRA, EPP, ADA and ECPA plus best practices for privacy and background screening, employee testing, workplace monitoring, employee investigation and termination of employment.

B. Please state the perceived need for the funds and how the applicant identified such need.

Few Assistant Attorneys General have formal training in the field of privacy and data security. Currently, only a group of AAGs in California and one AAG in Missouri have CIPP/US certifications. It is becoming more common to see attorneys representing targets of our investigations with this certification, and the knowledge gap in the area of privacy between AAGs and defense counsel may impair our ability to effectively investigate data security and privacy issues, and to craft appropriate remedies.

While most AAGs are well acquainted with their own states' privacy and data breach laws, and many are acquainted with HIPAA and other federal laws, it is becoming increasingly important for us to understand the entire privacy framework in which the targets of our investigations operate, both so that we can determine the best policies when negotiating AODs, and so that we speak with knowledge when communicating with our counterparts representing businesses, who are becoming increasingly sophisticated in this field.

CIPP Certification requires taking two exams: a general exams which covers foundations of privacy law, and a subject matter specific exam, in this case covering U.S. laws (other certifications are focused on Canada, Europe, IT, and professionals operating within the federal government). The total cost for the two required exams is \$550. Training for the exams costs \$1,195 (\$195 for books, \$950 for approximately 13 hours of online training, and \$50 for practice tests). IAPP has agreed to lower the cost of training to \$500 if at least 25 participants agree to take the exam, making the total cost of certification \$1,050 per participant.⁵

The TJX Grant funds would cover the full training and exam costs (\$1,050) for any member of an AGO who requests the funds.⁶ The final sum would be determined once we have a full count of interested AAGs. As a general matter, AGOs do not have the resources to reimburse this certification, and the cost is often too high for an individual AAG. Both AAGs and investigators would benefit from this training. The grant would *not* cover the \$100/year membership in IAPP, which each recipient would be

⁵ Some AAGs with existing CIPP/US certification may wish to pursue the CIPP/IT or CIPP/G (for U.S. Government) certifications. Because they have already passed the preliminary, general exam, they would only require half the funds, for the subject-matter specific exam and related training.

⁶ If the TJX Committee finds it appropriate, recipients of these funds could be required to agree to reimburse the training funds if they leave their offices within a year of receiving the certification.

required to pay

- C. If the application concerns an investigation and/or potential litigation please describe the investigation and/or litigation.**

This application does not apply to an individual investigation, but the training and certification would assist in every privacy and data breach matter in which the AGOs are involved.

- D. Please provide a detailed itemization of all expected costs and expenses related to the proposed project to be paid from the grant. (If applicable, include a description of how other elements such as volunteer labor or collaboration with other agencies will be integrated into the project.)**

The costs and expenses related to the proposed project will be as follows:

- The cost of each exam (Certification Foundation and Subject Matter Specific) is \$275, for a total of \$550.
- The cost of books, online training, and practice tests is a reduced rate of \$500.

The total cost for each AGO employee taking an exam will be \$1,050. If twenty-five AGO employees will participate in the project, the total cost will be \$26,250. If fifty AGO employees participate, the cost will be \$52,500.

- E. Please provide a detailed description of goods and services, such as personnel, travel and transportation, and materials to be used in connection with the proposed project that are funded from sources other than this grant.**

There are no additional sources of funding. Participants will use any office resources that their individual AGOs permit (computers, travel to the test sites, time to study, etc.)

- F. Please state the name, address, and telephone number of each source of funds (other than this grant) expected to be used in connection with the proposed grant project.**

There are no additional sources of funding.

- G. Please provide a description of how the applicant: (1) will ensure that distribution by the Data Security Fund Committee will be used solely for purposes proposed in the Application; and (2) intends to report to the Data Security Fund Committee concerning the results of the grant, including a discussion of how the applicant intends to measure the success of the grant (e.g., if the application is to retain an expert to**

assist in litigation, how does the applicant anticipate it will use the expert's assistance?). Appropriate non-staffing costs for such measurement may be included in the monies sought by the application.

If the TJX Committee preliminarily approves this application, the VT AGO, with the assistance of NAAG for coordination, will determine which individuals will participate in the program by contacting the Consumer Protection or Privacy chiefs in the Participating States, and by contacting offices through the Privacy Working Group mailing list. Once the number of applicants is determined, the TJX Committee will determine if the final cost is acceptable, and if so, the VT AGO will coordinate with IAPP for submission of the CIPP applications. We propose that the final cost of the project be paid directly by the TJX Committee to IAPP. If this is not possible, Vermont will seek authority to accept the funds from the TJX Committee, and then send those funds to IAPP. IAPP will arrange for delivery and setup of the materials and training.

Participants will be given six months to complete the training and take the tests. At the end of the period, the VT AGO will report to the Committee who took the exams and the pass rate. Any participants who fails an exam will be responsible for paying any costs relating to retaking the exam from their own resources.⁷

H. If the application is for continuation of a grant approved during a previous grant cycle, please describe the steps taken by applicant to determine the efficacy of the program during the prior grant cycle.

This is not a continuing grant.

IV. REPRESENTATIONS BY APPLICANT

A. Requests for Staff Expenses

Grants from the Data Security Fund are not available for staff expenses absent extraordinary circumstances. If the application includes a request for staff expenses, such as funding for salary or benefits, please provide a detailed explanation of the extraordinary circumstances justifying your request.


This application does not request staff expenses.

⁷ The Committee may wish to consider a requirement that any recipient who does not take the exam within six months must reimburse the committee for the cost of the training and exams.

B. Authority and Use of Funds

The undersigned is the responsible person for this Application, has been duly authorized by the Applicant to act as its agent in connection with this application, and hereby certifies that the information in this Application, including attached documents, is true. The undersigned has read the governing documents regarding the Data Security Fund that resulted from the multi-state investigation and understands their terms. The undersigned further represents that the funding requested will not be used to pay for regular staff of the agency or entity applying for this grant, and that the existing budget of applicant will not be reduced should the application be approved.

Signed:



Name:

Ryan Kriger

Title:

Assistant Attorney General

Return six (6) copies of Application and any attachments to:

Data Security Fund Committee
Attention: Lois Martin, Paralegal
Office of the Massachusetts Attorney General
Consumer Protection Division
One Ashburton Place
Boston, MA 02108



International Association
of Privacy Professionals

PRIVACY TRAINING PROGRAMS

The International Association of Privacy Professionals (IAPP) offers seven privacy and data protection training programs for organizations seeking to extend privacy knowledge to staff. Each of these programs is based on the comprehensive and up-to-date bodies of knowledge for the IAPP's Certified Information Privacy Professional (CIPP) designations.

The programs can be tailored to meet the individual needs of your organization by combining units from different programs. In addition, the IAPP professional training faculty member assigned to your organization will discuss your specific privacy issues and incorporate the information in the training program to the extent possible.

Program I: Foundation

(An introduction to major laws and concepts in privacy)

Unit 1 Common Principles and Approaches to Privacy

This unit includes a brief discussion of the modern history of privacy, an introduction to types of information, an overview of information risk management and a summary of modern privacy principles.

Unit 2 Jurisdictions and Industries

This unit introduces the major privacy models employed around the globe and provides an overview of privacy and data protection regulation by jurisdictions and by industry sectors.

Unit 3 Information Security: Safeguarding Personal Information

This unit presents introductions to information security, including definitions, elements, standards and threats/vulnerabilities, and to information security management and governance, including frameworks, controls, cryptography, and identity and access management (IAM).

Unit 4 Online Privacy: Using Personal Information on Websites and with Other Internet-related Technologies

This unit discusses the web as a platform and privacy considerations for sensitive online information, including policies and notices, access, security, authentication, identification and data collection. Additional topics include children's online privacy, e-mail, searches, online marketing and advertising, social media, online assurance, cloud computing and mobile devices.



International Association
of Privacy Professionals

PRIVACY TRAINING PROGRAMS

Program II: U.S. Private-sector Privacy

Unit 1 Introduction to the U.S. Privacy Environment

This unit covers the structure of U.S. law, the enforcement of U.S. privacy and security laws and information management from a U.S. perspective.

Unit 2 Limits on Private-sector Collection and Use of Data

This unit examines limits in the medical, financial, education and telecommunications and marketing sectors, as well as cross-sector privacy protection by the Federal Trade Commission.

Unit 3 Government and Court Access to Private-sector Information

This unit introduces privacy law and practice in law enforcement, national security and civil litigation.

Unit 4 Workplace Privacy

This unit includes an introduction to workplace privacy and more detailed privacy considerations before, during and after employment, including background checks, employee monitoring, investigation of employee misconduct and termination of the employment relationship.

Unit 5 State Privacy Laws

This final section of the U.S. private-sector privacy program examines U.S. state laws related in marketing, financial data, data security and breach notification.

Program III: Canadian Privacy

Unit 1 Canadian Privacy Fundamentals

This unit provides an introduction to the Canadian legal system, including laws and their interpretation and enforcement agencies and powers; privacy basics from a Canadian perspective and the underlying framework for Canadian privacy law and practice.

Unit 2 Canadian Privacy Laws and Practices—Private Sector

This unit explains the Canadian statutes related to privacy in the private sector, including PIPEDA, PHIPA and related provincial law.

Unit 3 Canadian Privacy Laws and Practices—Public Sector

This module discusses key concepts and practices related to The Privacy Act of Canada.



PRIVACY TRAINING PROGRAMS

Program IV: European Privacy

Unit 1 Introduction to European Data Protection

This unit introduces the origins and historical context for privacy in Europe, the European regulatory institutions and the legislative framework for current EU data protection law at both the EU and state level.

Unit 2 European Data Protection Law and Regulation

This unit takes an in-depth look at data protection concepts, application of the law, data protection principles, legitimate processing criteria, information provision obligations, data subject rights, confidentiality and security, notification requirements, international data transfers, and supervision and enforcement.

Unit 3 Compliance with European Data Protection Law and Regulation

This unit examines the employment relationship, surveillance activities, marketing activities, Internet technology and communications, and outsourcing.

Program V: U.S. Government Privacy

Unit 1 U.S. Government Privacy Laws

This unit reviews U.S. Government privacy definitions and principles and proceeds to review key laws and regulations for federal practice. It continues with a discussion of privacy and the federal government intelligence community and concludes with a review of other federal information privacy laws and authorities affecting government practice.

Unit 2 U.S. Government Privacy Practices

This unit applies information about the laws to privacy program management and organization, records management, and auditing and compliance monitoring.

Program VI: Privacy in Information Technology

Unit 1 Understanding the Need for Privacy in the IT Environment

This unit presents foundation elements for embedding privacy in IT, and provides an introduction to the information life cycle and common privacy principles.



PRIVACY TRAINING PROGRAMS

- Unit 2 **Privacy Considerations in the Information Life Cycle**
This unit discusses key considerations in the collection, use, disclosure, retention and destruction of personal information.
- Unit 3 **Privacy in Systems and Applications**
This unit introduces common challenges in the enterprise IT environment, identity and access management, credit card information and processing, remote access, data encryption, other privacy-enhancing technologies and special considerations for customer-facing applications.
- Unit 4 **Privacy Techniques**
This unit presents authentication techniques and degree of strength, identifiability and Privacy by Design (and re-design)
- Unit 5 **Online Privacy Issues**
This unit focuses on specific requirements for the online environment, corporate website design, common types of websites with a focus on sites that present a higher level of privacy challenges, online threats and e-Commerce personalization
- Unit 6 **Technologies with Privacy Considerations**
This unit discusses recent technologies with privacy implications, including cloud computing, wireless IDs, business intelligence and analytics, telecommuting, location-based services and bringing a personal computer to work. It concludes with emerging technologies, including smart grid, smart medical devices, video/data/audio surveillance and facial-recognition.

Program VII: Privacy Management (available Q1 2013)

- Unit 1 **Privacy Program Governance**
This unit describes how to create a privacy program at an organizational level, develop and implement a framework and establish metrics to measure program effectiveness.
- Unit 2 **Privacy Operational Life Cycle**
This substantial unit reviews privacy program practices through the privacy life cycle: assess, protect, sustain and respond.