CONTRACT USER GUIDE

How to Use the PRF56DesignatedOSC Statewide Contract Audit, Accounting, Compliance, Security and Revenue Recovery Services

Category: Information Management, Security and Compliance Audits Including Payment Card Industry (PCI) Data Security Standards (DSS) Compliance

Contract #: PRF56DesignatedOSC **Contract Duration:** 5/20/2013 to 6/30/2016

Options to renew: 3 at 1 year each through June 30, 2019

MMARS #: MAOSDPRF56DesignatedOSC – Must be used by State Departments on MMARS

Contract Manager: Howard Merkowitz, Deputy Comptroller -

Contract Manager Email: PRF56DataSecurity@massmail.state.ma.us

This contract contains: Supplier Diversity Program requirements, Prompt Payment Discounts

Last change date: 5/20/2013 initial issue date. Updated 6/6/2013.

Contract Summary

This Statewide Contract provides a full suite of compliance audits, quality assurance reviews and testing for information management systems and procedures, security management systems and procedures, including Payment Card Industry (PCI) compliance, other information security audits, compliance reviews of standards, and systems and controls to protect personally identifiable information and other sensitive data. Includes all types of audits, compliance and quality assurance reviews and testing for information and data management systems (paper or electronic), security compliance, Executive Order 504 compliance validation, PCI compliance, physical and electronic security of records, PII and confidential information, E-discovery, data breach forensics investigations and remediation, or other audits and compliance reviews related to data management systems and security.

This Statewide Contract has pre-qualified contractors approved by the Payment Card Industry Council to provide Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) services as well as other data management and data security audit professionals. As this Statewide Contract is procured under the authority of the Office of the Comptroller (CTR) to implement state finance law and prescribe fiscal accountability, State Department merchants must use this Statewide Contract to procure the services of QSA professionals and ASVs for Payment Card Industry Council Data Security Standards and for other information management security compliance audits (in any branch of government) as prescribed in the Non-Tax Revenue - Revenue Collection Data Security Policy. These services may not be independently procured under separate general procurement authority.

Contractors are listed for each of the following categories:

A. **PCI Council Approved Quality Security Assessors (QSAs) and related QSA Consulting Services.** Only Approved QSAs can perform PCI Compliance validation. QSAs are also qualified to provide other audit, compliance review and consulting services for non-PCI related compliance audits and reviews.

B. **PCI Council Approved Scanning Vendors (ASVs) and other Scanning and Compliance and Vulnerability Testing and Security Compliance Scans and Testing.** Only Approved ASVs can perform PCI Compliance validation. ASVs are also qualified to provide scanning and other testing and compliance services for non-PCI related compliance audits.

C. **Other Non-PCI Audit, Internal Control, Security And Compliance Audits And Reviews For General Information Management And Security Compliance.** Full range of audit, compliance reviews and related consulting services for non-PCI related compliance services for Executive Order 504 compliance validation, physical and electronic security of records, PII and confidential information, E-discovery, data breach investigations and remediation, compliance with ITD Enterprise Data Security and other enterprise or Eligible Entity data security policies, G.L. c. 93H and c. 93I PII security statutes, or other audits and compliance reviews related to data management systems, and security or Personally Identifiable Information (PII) and other types of confidential and sensitive information. QSAs are qualified under this Category to provide other audit, compliance review and consulting services for non-PCI related compliance audits and reviews.

Duration of Statewide Contract

The initial duration of the Contract is three (3) years through June 30, 2016, subject to continued successful performance. CTR reserves the right to negotiate any part of the RFR or contract to ensure continued best value for the Commonwealth, including scope and fees.

This Statewide Contract also has three (3) additional one (1) year options to renew, through June 30, 2019, subject to appropriation, continued successful performance, and the satisfactory renegotiation of each subsequent year's performance specifications. Subsequent year pricing will not increase substantially from the initial 3 year contract duration.

Engagements under a Statement of Work (SOW) may be "entered" into at ANY time PRIOR to the end date of the Contract for an authorized Vendor, even if the period of the SOW extends beyond the end date of the Statewide Contract. For State Departments using MMARS and an MA, if a transaction override is needed to encumber funds for engagements entered into prior to the end date of the Contract but extending beyond the end date, the Department should work with the CTR Contracts Bureau to facilitate the encumbrance and contract PRF56DataSecurity@massmail.state.ma.us to validate the use of the Statewide Contract for an engagement.

Vendors are required to support any transition of SOWs and to close out any SOW at the direction of the Eligible Entity, including returning any reports, data or other information used during performance and submitting any final deliverables in accordance with the SOW engagement terms.

How To Use this Statewide Contract

Summary of Where to Obtain Important Contract Information

Vendors and Eligible Entities are required to comply with and perform the duties, responsibilities and requirements as outlined under this Statewide Contract. Any of the terms contained in this document may not be amended or modified in writing or by actions or performance without prior written approval of the Office of the Comptroller (CTR). Past practice that does not comply with these specifications shall not be grandfathered.

Eligible Entities can contact any of the Vendors on the Contract to inquire about using their services. The Approved Vendors are located on the "Vendors" page of the contract on Comm-PASS. Click on the eyeglass icon to the right of

each Vendor's name to view its qualifications and contact information. At the bottom of the page for each Vendor click on the eyeglass icon to view its pricing. No additional contract documents are required to establish the referral relationship. **Eligible Entities may not sign any additional Vendor documents.**

To start the acquisition process of services, please download the Statewide Contract documents:

1. Go to the www.comm-pass.com website, click on the "Contracts" tab;
2. Select "**Search for Contract**" (or click this link: **Search for a Contract**);
3. Enter "**PRF56**" in the "Document Number" field and search.

Document Number: PRF56

The relevant documents necessary for use of this Statewide Contract are specified below in the order of contract precedence. All Eligible Entities using this Statewide Contract are required to comply with these terms.

	Hierarchy of Contract Documents (Order of Precedence)	Documents available on www.Comm-PASS.com Under PRF56DesignatedOSC Statewide Contract
1	Commonwealth Terms and Conditions (each Vendor has executed)	"Forms and Terms" tab Contact CTR for Executed Copy
2	Standard Contract Form (each Vendor has executed)	"Forms & Terms" tab Contact CTR for Executed Copy
3	Request for Response (RFR) PRF56DesignatedOSC (Bid document) as amended, including the approved Statement of Work (SOW)/Quote Form published under this Contract.	"Forms & Terms" tab
4	Contract User Guide Including Additional Terms and Authorized Clarifications	"Forms & Terms" tab
5	Contractors Response Document, including pricing, as amended by Best and Final Offers or Negotiations and any responses to the approved Statement of Work (SOW) Form published under this Contract for a particular engagement, including any other non-conflicting provisions, terms or materials incorporated herein by reference by the Contractor.	"Vendor" tab for each specific Vendor

Requirements for Competitive Quotes

1. **PRF56 Data Security Statement of Work (SOW)/Quote Form.** For purposes of this Statewide Contract, Eligible Entities are required to pre-populate the **PRF56 Data Security Statement of Work (SOW)/Quote Form** posted on www.comm-pass.com for this contract with the proposed work to be performed under an engagement. For Statewide Contract management purposes, for State Departments users, Vendors are required to notify CTR by email to: PRF56DataSecurity@massmail.state.ma.us when a new engagement has begun, and CTR may request periodic reports of all engagements at any time from Eligible Entities and Vendors.

2. **Competitive Quotes.** The pre-populated **PRF56 Data Security Statement of Work (SOW)/Quote Form** should be sent by email by the Eligible Entity to multiple Contractors authorized for the category of performance sought, unless the Eligible Entity is currently engaged for the same work under prior engagement with one of the awarded Vendors. Eligible Entities are encouraged to submit quotes to all Contractors in a category to obtain the broadest range of performance and competition. Note that Contractors are authorized to provide performance solely in their authorized performance categories.

3. The **PRF56 Data Security Statement of Work (SOW)/Quote Form** is then returned completed (unexecuted) by email from the Contractors interested in bidding on the engagement to the Eligible Entity.

4. The Eligible Entity reviews the **Contractor's Response Document including pricing (#5 in hierarchy of documents above)** along with the **PRF56 Data Security Statement of Work (SOW)/Quote Form** to select the best value Contractor for the engagement. Selection may include interviews and negotiations to finalize the engagement performance terms and pricing. Pricing for any SOW engagement may not be greater than prices

posted under the Contract and Contractors are limited to providing only the services within the authorized category(ies) for that Contractor.

5. **Updated/Finalized SOW**. Once a Contractor has been selected, the details of the engagement (services to be performed, timeline or schedule of performance completion dates and pricing) should be finalized by updating the SOW that is executed by authorized signatories of the Vendor and Eligible Entity. Eligible Entities may request a copy of the Contractor Authorized Signatory Listing (CASL) from CTR at PRF56DataSecurity@massmail.state.ma.us that is used to validate authorized signatories for a Contractor. The SOW is not a separate contract but an engagement under the Statewide Contract PRF56DesignatedOSC incorporated by reference herein, and serves as the scope of performance and budget for this engagement. Additional conflicting contract terms and conditions may not be included, referenced or attached to the SOW.

6. **Materials Incidental to the Service.** As this is an audit service, Eligible Entities will negotiate the scope of the engagement and provide access to the systems, protocols, staff and information necessary to perform the audit. Eligible Entities, depending upon the engagement, may be asked to identify team and primary contacts, payment data flow, network diagram, outward facing IP addresses and wireless networks, identify if the Eligible Entity is using its own payment application or a third-party application, policies and internal controls for maintaining information security and data security compliance.

7. **Contract File Additional Documents.** Copies of the Commonwealth Terms and Conditions, Standard Contract Form, Contractor Authorized Signatory Listing (CASL), Prompt Payment Discount Terms (in SCF) are available from CTR and can be emailed to an Eligible Entity upon request to complete the Contract File (for audit purposes) and to validate signatories when executing SOWs. Please email PRF56DataSecurity@massmail.state.ma.us for these documents, and with any questions related to using the SOW and Statewide Contract.

8. **Purchase Options**: Bidders will be paid based upon reaching established scheduled milestones, submission of required reports, data or other documentation in accordance with required scope of service and fees. Eligible Entities reserve the right to withhold payment for any scheduled milestone that is not met until properly completed. Eligible Entities also reserve the right to apply a retainage on all payments to ensure delivery of services under the terms of the contract.

9. **Payments by State Departments.** All payments made by State Departments under the state accounting system MMARS MUST be made using the Master Agreement (MA) for this Statewide Contract: **MAOSDPRF56DesignatedOSC.**

10. **Additional Reporting Requirements for Contract Management.** For Statewide Contract management purposes CTR may request periodic reports of all engagements under the Statewide Contract at any time from Eligible Entities and Vendors.

General Background

Payment Card Industry Council Security Standards for Acceptance of Credit and Debit Cards

All Commonwealth Entities that currently accept credit or debit card payments are considered “merchants” and are required to validate data security compliance. Compliance standards are set by the Payment Card Industry Council and compliance is enforced by the payment card brands for each merchant level, which depends upon the volume of transactions.

The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC) and its founders, the global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

The PCI Data Security Standard and supporting documents represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information. The standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents. To reduce the risk of compromise and mitigate its impacts if it does occur, it is important that all entities storing, processing, or transmitting cardholder data be compliant.(https://www.pcisecuritystandards.org/security_standards/index.php)

Any Commonwealth Department that accepts credit or debit cards is required to comply with the merchant requirements published by the Payment Card Industry Council in addition to any other state or federal laws, regulations or policies related to the storing, processing or transmitting of cardholder data which is considered PII. Depending on the Department's merchant level and volume of transactions, a Department may be required to complete a PCI DSS Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC) and file with their merchant bank, conduct quarterly vulnerability scans, penetration tests and facilitate periodic validation of Payment Card Industry Data Security Standards compliance.

Data Security compliance helps merchant Eligible Entities improve the safekeeping of cardholder information by tightening overall security standards and information management to:

- Minimize vulnerabilities;
- Reduce the chance of breaches, fraud, and financial loss;
- Ensure the security of the Commonwealth of Massachusetts' public facing e-commerce applications; and
- Reduce the scope of audit requirements by reducing the scope of potential data breaches or system and protocol vulnerabilities.

In addition, the Commonwealth of Massachusetts, pursuant to Executive Order 504, G.L. c. 93H and 93I has responsibility to safeguard data deemed Personally Identifiable Information (PII), in addition to protections mandated by other state and federal statutes and regulations for other types of confidential data.

The duties to protect PII under Executive Order 504, G.L. c. 93H and 93I and other authority apply equally to both PCI covered data (credit card holder data) and non-PCI covered data (bank accounts, ACH and all other personally identifiable information (PII)). At this time, the Payment Card Industry Council mandates a formal PCI Compliance process to validate DSS for all merchants. For Executive Departments governed by Executive Order 504, an Enterprise self-assessment process has been completed to document the types of confidential and PII data collected and retained by Departments, and the Information Technology Division (ITD) has published Enterprise Security Standards for the protection of confidential, sensitive and PII. The services available under this Statewide Contract can be used to audit compliance under these mandates.

By policy, the Office of the Comptroller and the Information Technology Division (ITD) have mandated that all Commonwealth Department merchants provide annual certification of Data Security compliance even if an independent audit is not required by the Payment Card Council or the Eligible Entity (merchant's) acquiring bank. See Non-Tax Revenue – Revenue Collection Data Security Policy. This additional requirement is necessary to ensure that Department merchants are taking the necessary steps to annually verify continued Data Security compliance and have an

independent evaluation that vulnerabilities have been identified and mitigated to prevent a data breach under G.L. c. 93H and c. 93I or the Payment Card Industry Council standards.

Annual budgets for any Eligible Entity accepting revenue should ensure sufficient funding to maintain continued data security compliance, and reduction in budgeted funds will not support any failure to maintain continued compliance.

Benefits and Cost Savings

- **Contractor Competition** – The Contract provides access to multiple qualified Statewide Contractors in each of the data security categories each with a variety of experience and services and with competitive rates.
- **Bidder Qualification** – The Strategic Sourcing Services Team (SSST) reviewed each bidder's qualifications to select the most competitive pool of data security experts. Selected Contractors demonstrate leading industry standards in technology, security, Payment Card Industry (PCI) compliance and other protocols to ensure the highest level of security and privacy in the transmission, acceptance and handling of data.
- **Standard Procurement** – This Contract provides seven (7) Vendors to perform the services under the Contract for the duration of the procurement. For the lifetime of the procurement CTR reserves the right to select additional Contractors from the original procurement, for additional work as warranted or to re-open the procurement to procure additional or replacement Contractors.

Vendor List and Contract Information

The awarded Contractors are listed below. Please refer to the "Vendor" tab of Comm-PASS (www.comm-pass.com) at the bottom of the vendor detail page for the "Contractors Pricing Information" attachment. Supplier involvement in any of the following programs will have the appropriate icon appearing on the "Vendor" tab page in Comm-PASS. Programs include Small Business Purchasing Program (SBPP), Supply Diversity Office Certification (SDO, formerly SOMWBA Certification), Supplier Diversity Program (SDP, formerly AMP).

Awarded Vendors – Quality Security Assessors (QSAs) – Eligible Entities

PCI Council Approved Quality Security Assessors (QSAs) and related QSA Consulting Services. Only Approved QSAs can perform PCI Compliance validation. QSAs are also qualified to provide other audit, compliance review and consulting services for non-PCI related compliance audits and reviews.

Eligible Entities are required to submit the Statement of Work (SOW)/Quote Form by email to **at least two (2) Awarded Vendors** unless the Eligible Entity is currently engaged for the same work under prior engagement with one of the awarded Vendors.

Eligible Entities are encouraged to submit quotes to all Contractors in a category to obtain the broadest range of performance and competition. Note that Contractors are authorized to provide performance solely in their authorized performance categories.

	PCI Council Approved Quality Security Assessors (QSAs) QSA Vendors (PCI and Non-PCI)	Contact	Email Address	Phone Number
1	Coalfire Systems, Inc.	Joseph Krause	joe.krause@coalfire.com	508-347-5282
2	Compass IT Compliance LLC	William DePalma	wdepalma@compassitc.com	401-353-3024
3	FishNet Security, Inc.	Jarrett Black	jarrett.black@fishnetsecu	978-392-2111x8005

	PCI Council Approved Quality Security Assessors (QSAs) QSA Vendors (PCI and Non-PCI)	Contact	Email Address	Phone Number
			rity.com	
4	Verizon Business Network Services Inc	Andi Baritchi	andi.baritchi@verizon.com	972-489-4289

Awarded Vendors – Approved Scanning Vendors (ASVs)

PCI Council Approved Scanning Vendors (ASVs) and other Scanning and Compliance and Vulnerability Testing and Security Compliance Scans and Testing. Only Approved ASVs can perform PCI Compliance validation. ASVs are also qualified to provide scanning and other testing and compliance services for non-PCI related compliance audits and reviews.

Eligible Entities are required to submit the Statement of Work (SOW)/Quote Form by email to **at least two (2) Awarded Vendors** unless the Eligible Entity is currently engaged for the same work under prior engagement with one of the awarded Vendors.

Eligible Entities are encouraged to submit quotes to all Contractors in a category to obtain the broadest range of performance and competition. Note that Contractors are authorized to provide performance solely in their authorized performance categories.

	PCI Council Approved Scanning Vendors (ASVs) and other Scanning, Compliance and Vulnerability Testing and Security Compliance Scans and Testing ASV Scanning Vendors (PCI and non-PCI)	Contact	Email Address	Phone Number
1	Akibia, Inc – d/b/a Zensar Technologies IM, Inc.	Jim Spencer	jspencer@akibia.com	508-304-4409
2	Coalfire Systems, Inc.	Joseph Krause	joe.krause@coalfire.com	508-347-5282
3	Compass IT Compliance LLC	William DePalma	wdepalma@compassitc.com	401-353-3024
4	FishNet Security, Inc.	Jarrett Black	jarrett.black@fishnetsecurity.com	978-392-2111x8005

Awarded Vendors – Non-PCI Audit, Internal Control, Security Compliance Audits

Other Non-PCI audit, internal control, security and compliance audits and reviews for general information management and security compliance. Full range of audit, compliance reviews and related consulting services for non-PCI related compliance services for Executive Order 504 compliance validation, physical and electronic security of records, PII and confidential information, E-discovery, data breach investigations and remediation, compliance with ITD Enterprise Data Security and other enterprise or Eligible Entity data security policies, G.L. c. 93H and c. 93I PII security statutes, or other audits and compliance reviews related to data management systems, and security or Personally Identifiable Information (PII) and other types of confidential and sensitive information. QSAs are qualified under this Category to provide other audit, compliance review and consulting services for non-PCI related compliance audits and reviews.

Eligible Entities are required to submit the Statement of Work (SOW)/Quote Form by email to **at least three (3) Awarded Vendors** unless the Eligible Entity is currently engaged for the same work under prior engagement with one of the awarded Vendors.

Eligible Entities are encouraged to submit quotes to all Contractors in a category to obtain the broadest range of performance and competition. Note that Contractors are authorized to provide performance solely in their authorized performance categories.

	Other Non-PCI audit, internal control, security and compliance audits and reviews for general information management and security compliance. Non-PCI Data Security Audit Vendors	Contact	Email Address	Phone Number
1	Coalfire Systems, Inc.	Joseph Krause	joe.krause@coalfire.com	508-347-5282
2	Compass IT Compliance LLC	William DePalma	wdepalma@compassitc.com	401-353-3024
3	Deloitte & Touche, LLP	Kiran Mantha	kmantha@deloitte.com	212-362-1236
4	Ernst & Young U.S., LLP	Francis Nemia	francis.nemia@ey.com	617-585-3496
5	FishNet Security, Inc.	Jarrett Black	jarrett.black@fishnetsecurity.com	978-392-2111x8005

Who Can Use This Contract?

Applicable Procurement Law: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00

Eligible Entities:

01. Cities, towns, districts, counties and other political subdivisions;
02. Executive, Legislative and Judicial Branches, including all Eligible Entities and elected offices therein;
03. Independent public authorities, commissions and quasi-public agencies;
04. Local public libraries, public school districts and charter schools;
05. Public Hospitals, owned by the Commonwealth;
06. Public institutions of high education;
07. Public purchasing cooperatives;
08. Non-profit, UFR-certified organizations that are doing business with the Commonwealth;
09. Other states & territories with no prior approval by the State Purchasing Agent or Office of the Comptroller required;
10. Other entities when designated in writing by the Office of the Comptroller.

Strategic Sourcing Services Team (SSST) Members

DEPARTMENT	Strategic Sourcing Services Team (SSST) Members
Office of the Comptroller	Howard Merkowitz
Office of the Comptroller	Julie Burns
Office of the Comptroller	Jenny Hedderman
Office of the Comptroller	Tom Shack

DEPARTMENT	Strategic Sourcing Services Team (SSST) Members
Office of the Comptroller	Howard Merkowitz
Office of the Comptroller	Tim O'Neill
Office of the Comptroller	Patricia Davis
Office of the Comptroller	Monica Middleton
Dept. of Conservation & Recreation	Kent Carlson
Dept. of Elementary & Secondary Education	Kalyanakumar Thirumalasamy
Dept. of Public Health	Phil Wiswell
Dept. of Transportation	Silvio Petraglia
Exec Office of Energy & Environmental Affairs	Lonsdale Koester
Exec Office of Health & Human Services	Alice Kyeba
Exec Office of Health & Human Services	Nilsa Morales
Information Technology Division	Kevin Burns
Middlesex Community College	Alan Keniston
Trial Court	Mary Donovan
Operational Service Division	William Funk

Specifications That Apply To All Eligible Entities and Contractors

The following specifications apply to both Vendors and Eligible Entities for use of this Statewide Contract and have been added to clarify the responsibilities of Eligible Entities and authorized Statewide Contractors relative to Statewide Contract PRF56DesignatedOSC. Any terms submitted as part of the procurement process have been reviewed and considered and the following terms have been approved as authorized clarifications. All other terms or attachments submitted as part of the procurement (e.g., identifying warrantees, limitations of liability, copyright or other terms) that have not been specifically identified below have been considered, but not accepted under this Contract.

These terms apply solely to this Statewide Contract and create no precedent for any other engagement outside of PRF56DesignatedOSC. These terms are incorporated by reference into the PRF56DesignatedOSC Statewide Contract and shall apply to any engagement Statement of Work (SOW) entered into between an Eligible Entity of the Commonwealth of Massachusetts and an authorized Statewide Contractor under PRF56DesignatedOSC.

Contractors have agreed by submission of an RFR Response under this Statewide Contract that they have accepted the hierarchy of documents and order of precedence identified in this Section and that any terms forms or other agreement made with any Eligible Entity will be considered void or voidable by the Commonwealth and shall not be binding upon any Eligible Entity, even if services have been accepted under this Statewide Contract.

A Contractor may not require any additional agreements, engagement letters, contract forms, click through agreements, or any other mandatory or automatic additional terms as part of the Statewide Contract that have not been approved by the Office of the Comptroller and any document executed by an Eligible Entity may be deemed void or voidable by the Commonwealth.

Additional non-conflicting terms related to service performance details, that comply with the required terms of the RFR, may be added to a Statement of Work (SOW) engagement, as published for this Statewide Contract, provided the intent or effect of the language does not supersede or replace the language of the Contract and this Contract User Guide.

1) Contact Information and Key Personnel

a) Vendors must ensure that contact information is accurate. The person and address listed on the Vendor Tab on www.Comm-PASS.com usually matches the Contract Manager and address identified in the Standard Contract Form for the Statewide Contract. Changes to the Contract Manager are considered changes to Key Personnel and will require a formal notice from an Authorized Signatory outlining the reason for the change and that the new individual is equally or more qualified than the current Contract Manager.

b) Corrections to email addresses, telephone or fax numbers are considered informal corrections. Vendors should email all change requests, as well as any additional email addresses they wish to be added for contact purposes to: PRF56DataSecurity@massmail.state.ma.us**.**

c) All notices, emails or other inquiries to CTR from Vendors or Eligible Entities should be sent to: PRF56DataSecurity@massmail.state.ma.us.

d) No subcontractor, agent or employee of a Vendor shall directly or indirectly supervise any employee of an Eligible Entity. For the purposes of the Statewide Contract "supervise" shall mean to direct the activities of an Eligible Entity employee on any basis, by direct, verbal or written communication from the Vendor to the employee, by indirect communication through a third-party or by any other means.

2) Fees and Pricing

A Vendor's fee and rate schedule under the Statewide Contract, shall remain in effect and unchanged for the initial duration of the Statewide Contract. These rates may not be re-negotiated to a higher rate with an individual Eligible Entity but may be negotiated down at any time. Rate schedules are posted on Comm-PASS for each Vendor.

3) Travel Time, Travel Expenses and Other Business Expenses

Expenses and travel associated with providing a quote are provided under the fee pricing posted for the contract. Consequently, Contractors may not charge Eligible Entities for expenses and travel associated with providing services except as authorized on the rate schedule for the Vendor approved under the Statewide Contract.

4) Statewide Contract Administration Fee and Report

This Statewide Contract shall **NOT** be subject to a 1% Contract Administration Fee, which is created pursuant to GL c. 7, § 3B, 801 CMR 4.02 and the Transaction Fee section in this solicitation and/or incorporated by reference into Statewide Contracts with the Operational Services Division (OSD).

5) Contacting Eligible Entities

Vendors may contact Eligible Entities about services offered under the Statewide Contract. Vendors may market only the services under the Statewide Contract and no other services or terms. Refer to the Commonwealth website for the following lists: Listing of Agencies, and the Listing of Cities and Towns.

6) Limitation of Liability for Information Technology Contracts

The language under this heading contained on Page 4 of the Standard Contract Form which incorporates by reference the Commonwealth Terms and Conditions, shall apply to this Contract. This language has been approved by the Office of the Attorney General and State Departments are not authorized to negotiate limits beyond this language. Contractors may not require or condition services on any Eligible Entity's negotiation or acceptance of any terms related to liability or indemnification and all such terms shall be deemed void by the Commonwealth.

7) Contract Termination or Suspension

Pursuant to the **Commonwealth Terms and Conditions**, Section 4. **Contract Termination or Suspension,** the Contractor shall be provided with prior written notice of any deficiencies and a reasonable opportunity to cure, prior to termination or suspension for cause, and a minimum of 30 days prior written notice under the notice language of the Standard Contract Form for any without cause termination unless the parties agree to a longer period of notice for termination or suspension under an SOW.

This section shall not apply to terminations or suspensions resulting from forced allotment reductions due to declining revenues pursuant to M.G.L. c. 29, § 9C or other legislative reductions or changes in spending authority or available funds. In the event an engagement is terminated without cause, an Eligible Entity shall negotiate all final costs with the Contractor which may include reasonable expenses and out-of-pocket costs incurred, including startup costs during the period up to and including the termination date. All final and close out performance shall be subject to review and acceptance by the Eligible Entity, which shall not be unduly delayed or unreasonably withheld. Travel costs and other similar charges are not compensable under the Contract, but are considered part of the blended rate and should not be billed separately unless approved in writing in advance of the obligation by the Eligible Entity and the amounts are included as part of a current SOW engagement. Costs must be adjusted accordingly since blended rates under this Contract are intended to include travel costs unless otherwise approved.

Upon termination or suspension, the Contractor may not be paid any amounts which exceed the value of the performance provided and accepted by the Eligible Entity and the Contractor under an executed SOW and the Contractor may not adjust invoices or accelerate payments in order to recoup the full value of performance not yet made under an SOW. The Contractor may terminate an engagement with 60 days prior written notice, or other period as negotiated by the parties and included in the SOW engagement, but may with 30 days prior written notice terminate an engagement if the engagement has may trigger an accounting standards or practices violation or other conflict.

8) Deliverables and Work Product

Each party agrees that, except and to the extent provided below, it shall acquire no right, title or interest in or to the other party's information, data base rights, data, tools, processes or methods, or any patents, copyrights, trademarks, service marks, trade secrets, or any other intellectual property rights of the other party by virtue of the provision or use of the Services and materials delivered pursuant to this Contract.

Eligible Entities acknowledge and agree that any advice, recommendations, information or Contractor owned work product provided to them by a Contractor in connection with performance of a deliverable under a SOW, including a security audit or evaluation engagement, is for the Eligible Entity's confidential and exclusive use and shall not automatically be deemed a public record if security or confidential information of the Eligible Entity is contained in these materials. The Eligible Entity will determine what records constitute a public record.

Independent audits of data or security systems may or may not be considered confidential depending upon the engagement and audit requirements for mandatory disclosure. If disclosure of an independent audit report is required, the Contractor shall disclose as required by audit disclosure obligations. For all other independent or other audits conducted solely for the Eligible Entity's internal controls and security assessment purposes shall not automatically be deemed a public record and shall be considered confidential and may not be disclosed or used for any purposes by the Contractor other than as authorized in writing by the Eligible Entity.

Except as otherwise required by the Public Records law or other applicable law, the Eligible Entity will not disclose or permit access to non-deliverables or other Contractor work product materials (which may include but not be limited to:

advice, recommendations, reports, information, software, analytics, algorithms, summaries, methodologies, or other Contractor-owned or proprietary materials) without Contractor's prior written consent. A Statement of Work (SOW) may include details of what materials or other non-deliverables may be disclosed.

All Eligible Entity data or other information contained in any reports created by the Contractor for the Eligible Entity shall remain the sole property of the Eligible Entity. Any Contractor owned Intellectual Property, including copyrighted information in such reports, shall remain the sole property of the Contractor and the reports shall not automatically be considered a "deliverable", provided however that the intellectual property is inextricable from the report or other product. Contractors may not attach trademarks, seals, proprietary materials, designs or other items to a deliverable solely to prevent the deliverable from being considered a deliverable or public record. All deliverables are considered public records unless the records contain confidential data of the Eligible Entity or a data subject, or meet another exception from disclosure under the Public Records Law or other state or federal law. Subject to Section 11 of the Commonwealth Terms and Conditions, the Eligible Entity will, subject to appropriation and within the limits imposed by law for claims against the Commonwealth or non-State Department Eligible Entity, indemnify Contractor for proven damages suffered by the Contractor resulting from unauthorized disclosure.

9) Intellectual Property, Copyright or Ownership Rights

The Contractor will retain any copyright or other ownership rights in the software, products, tools, definitions, questionnaires, research, training materials, and programs that are proprietary or owned by the Contractor prior to the date of the Statewide Contract. Deliverables, which include any item developed or provided to an Eligible Entity and paid for with Commonwealth or Eligible Entity funds will be presumed to be owned by the Commonwealth or Eligible Entity unless appropriate cost sharing or ownership rights are negotiated by the parties with fair market value provided to the Commonwealth or Eligible Entity, and amounts may be deducted from the performance costs of the Contractor to reflect any discounts for this fair market value, in addition to any other discounts including prompt paid discounts. A Commonwealth or Eligible Entity is not authorized to allow any Contractor to use, sell or profit directly or indirectly from the use of Commonwealth or Eligible Entity deliverables, which are deemed Commonwealth or Eligible Entity property, without just compensation or comparable discounts or in-kind performance.

Contractors shall own all right title and interest in and to Contractor trade secrets, confidential information or other proprietary rights, any ideas, information or other material owned by the Contractor prior to this Statewide Contract, or used or developed by the Contractor for performance which is not developed to be a deliverable under a SOW (such as software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications) that support the performance of deliverables, but are not a deliverable to be provided under a SOW.

Eligible Entities are prohibited from creating derivative works of all or any portion of any Contractor-owned property and are prohibited from reverse engineering, decompiling, disassembling, or otherwise attempting to discover source code of Contractor owned intellectual property or from copying, disclosing, or using Contractor owned property, except as otherwise provided in a SOW.

10) Confidential Information

All Contractors are subject to the enhanced privacy terms outlined in Executive Order 504, G.L. c. 93H and G.L. c. 93I, and any other applicable confidentiality requirements as outlined in the PRF56DesignatedOSC Statewide Contract. The Contractor will be notified at the time of a SOW engagement if the Contractor will be a holder or have direct or indirect access to personal or other restricted data. The Eligible Entity and the Contractor will outline in writing the protocols necessary to adequately secure this data which will be incorporated into the Statement of Work (SOW) engagement. Contractors shall treat all data received, accessed, created, transmitted, stored or processed as part of a SOW as

confidential and shall be responsible for the unauthorized disclosure or data breaches of any confidential data due to Contractor action or inaction.

11) Assignment.

Individual SOW engagements may not be assigned to a third-party, even if the third-party is a subsidiary of the Contractor, because participation in the Statewide Contract was competitively procured based upon the FEIN of the Contractor and third-parties have no right to benefit from an assignment without a competitive procurement. Subsidiaries and other third-parties may be used for performance under subcontracts provided the use of subcontractors is disclosed to and authorized by the Eligible Entity. Eligible Entities, in limited unusual circumstances, may authorize the assignment of a SOW engagement in accordance with Office of the Comptroller Contract Amendment policies, provided the Office of the Comptroller has approved the assignment under the Statewide Contract, which will not unreasonably be withheld if the assignment does not compromise the procurement requirements under the Statewide Contract. An Eligible Entity may not assign a SOW to another Eligible Entity unless the assignment is a result of the Eligible Entity being consolidated, abolished or otherwise having a material structural change or when funding has been transferred to another Eligible Entity and upon acceptance of the assignment by the Contractor.

12) Security Compliance Assessments (Non-PCI Data Security Audits)

The Commonwealth and Eligible Entities acknowledge and agree that: (i) any outcome of the services involving compliance assessment is limited to a point-in-time examination of the Commonwealth's or Eligible Entity's compliance or non-compliance status with the applicable standards or industry best practices set forth in the Scope of Work (SOW) and that the outcome of any audits, assessments or testing by, and the opinions, advice, recommendations and/or certification by Contractor does not constitute any form of representation, warranty or guarantee that the Commonwealth's systems are 100% secure from every form of attack, and (ii) in assisting in the examination of the Commonwealth's or Eligible Entity's compliance or non-compliance status, Contractor relies upon accurate, authentic and complete information provided by the Commonwealth or Eligible Entity as well as use of certain sampling techniques as negotiated by the parties.

13) Security Compliance Assessments (PCI Data Security Audits and Records Management)

For services under categories A and B for Payment Card Industry (PCI) compliance SOWs (PCI Council Approved Quality Security Assessors (QSAs) and related QSA Consulting Services, and PCI Council Approved Scanning Vendors (ASVs)):

The parties hereto recognize that changes to the Payment Card Industry Data Security Standard (PCI DSS) implemented subsequent to the date of an SOW may affect testing and reporting activities required for the services described therein. The parties agree that such changes, if implemented by the PCI Security Standards Council (PCI SSC), will be jointly reviewed by the parties and adjustments will be made if necessary, as mutually agreed to by the parties, to the activities and associated fixed-fee budget(s) described in the SOW to support those changes in accordance with PCI SSC requirements.

Moreover, all parties hereto agree that Contractor will have no liability for actions against the Commonwealth or Eligible Entity by Visa U.S.A., PCI SSC or PCI SSC's member organizations with respect to the Commonwealth's or Eligible Entity's PCI compliance based upon confidential information required to be contained in the any formal compliance attestation report subject to standards published by the PCI SSC (including, but not limited to, Report on Compliance, Report on Validation, ASV Vulnerability Scan Report, and other developed materials) provided the liability results solely from Commonwealth or Eligible Entity actions and the reports or other materials were accurate and complied with SOW requirements.

In addition to records management requirements under this Statewide Contract (which require maintaining all records related to performance for 6 years from the last payment under a SOW), Contractors may be required to comply with the record retention policies of the Payment Card Industry (PCI DSS) if the Eligible Entity accepts credit or debit cards for payments, including without limitation securing and maintaining digital and/or hard copies of case logs, audit results and work papers, notes, and any technical information that was created and/or obtained during the PCI DSS assessment for a minimum of three (3) years, or such longer period of time required to satisfy any applicable legal or regulatory requirements. All such information shall be held confidential in accordance with an SOW and this Statewide Contract. For the purposes of this section, the terms "Assessment" and "Requesting Organization" have the meaning ascribed to those terms in Appendix A of the PCI Security Standards Validation Requirements for Qualified Security Assessors, a copy of which is located at https://www.pcisecuritystandards.org and "Results" means the Report on Compliance and any associated working papers, notes and other materials and information generated in connection with an Assessment, including a copy of this Agreement. Notwithstanding any SOW between the parties to the contrary and to meet compliance requirements imposed by the PCI SSC, the parties understand and agree that, with prior notice and an opportunity to review any Results, the Contractor will be permitted to submit the Results of each Assessment to a Requesting Organization.