STATE OF VERMONT

INFORMATION TECHNOLOGY PROCUREMENT GUIDELINE

The Information Technology Guideline is provided as a companion to Administrative Bulletin 3.5 and carries the same authority.

ISSUED BY: Justin Johnson, Secretary of Administration

EFFECTIVE DATE: July 1, 2016

REVISION DATE: April 12, 2017

Hard copies of this document are considered uncontrolled. If you have a printed version, please refer to the OPC website at http://bgs.vermont.gov/purchasing-contracting/forms **for the official, in-force version.**

STATE INFORMATION TECHNOLOGY PROCUREMENT GUIDELINE

Table of Contents

STATE INFORMATION TECHNOLOGY PROCUREMENT GUIDELINE

1. Introduction; Purpose and Scope

This Guideline is designed to provide guidance to Agencies who are involved in the procurement of "information technology activities," as defined below. The goals of this Guideline are to establish a standard framework for the procurement of information technology activities, increase awareness of the numerous issues and risks Agencies may face when conducting IT procurements and to provide assistance for effectively addressing those issues and risks. This Guideline includes statutory requirements, policies, procedures and methods to promote best practices in securing necessary information technology ("IT") products and services for the State. This Guideline is not intended to cover every situation which may be encountered during IT procurement and contracting. Interpretation and application of this Guideline to unique situations is the responsibility of the Office of Purchasing & Contracting ("OPC").

Agencies must note that the use of non-State web-based systems (such as Dropbox, or Google applications), must be approved by the Secretary of Administration.

This Guideline is to be read together with Administrative Bulletin 3.5 and applicable State law which form a framework for conducting procurements and drafting, negotiating and enforcing contracts.

The Information Technology Procurement Guideline will be updated on an as needed basis as determined by OPC, DII and AGO due to changes in the technology industry, methodologies and offerings. The most current version of this Guideline will be posted on-line at: http://bgs.vermont.gov/purchasing-contracting/forms.

2. What's Different about IT Procurement & Contracting?

The procurement of IT products and services requires special diligence and the application of best practices to obtain secure, best-value IT solutions for the State. IT Products and services differ in complexity and analysis from other commodity and service procurements because technology is

constantly changing due to new service offerings, technical modifications and improvements, new delivery technologies and security concerns.

Information technology projects require appropriate planning, procurement processes, contract negotiation, project management and contract oversight in order ensure the State receives the technical functionality it needs within acceptable timeframe, budget and risk parameters.

Agencies must pursue a structured IT procurement process which provides a comprehensive framework to ensure:

- omissions from a business, technical or legal standpoint are anticipated and prevented;
- the costs and resources for the IT procurement process are appropriate and are efficiently deployed;
- the business case in support of the IT procurement is reaffirmed prior to selecting a solution;
- the project sponsor has confidence in the product selected as a result of user group involvement throughout the IT procurement process;
- risks have been appropriately considered; and
- the State has an acceptable exit strategy.

Regardless of the nature of the anticipated IT procurement, its size, cost and complexity, the following core principles of IT procurement apply:

- The procurement process should be justified by a comprehensive cost analysis that includes the total cost of ownership and all cost components including ongoing maintenance and not just the price of software or hardware.
- Use a structured procurement process that incorporates and balances concerns across Agency subject matter, technical and security experts, project management, Agency financial staff, Office of Purchasing & Contracting (OPC), Department of Information and Innovation (DII) and the Office of the Attorney General (AGO).
- Contract formation and negotiation are part of the decision process. It is important to include appropriate contract terms in the solicitation (RFP, RFQ, or simplified bid, etc). For purposes of IT contracting this may include business decisions around: location of data, intellectual property and software ownership, information security, confidentiality, service

and data availability requirements and other critical terms and conditions. It is equally critical to ensure that all RFP requirements are set forth in the resulting contract.

- Business needs must be supported in the solicitation of requirements and any contractual description of services.
- The nature of the data to be accessed, processed or stored must be assessed in order to include appropriate contractual provisions to address security, confidentiality, breach notification and data ownership.
- Long-term issues such as obsolescence, technology replacement and compatibility must be part of the evaluation, negotiation and decision-making process.
- Negotiations must be conducted prior to the execution of a contract with a particular IT solution or vendor; this may include negotiation of software license terms

3. Definitions

Unless otherwise defined herein, all terms used in this Guideline shall have the meanings set forth in Bulletin 3.5.

Availability means ensuring timely and reliable access to and use of data/systems.

Confidentiality means preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and Confidential Information.

Data Categorization means the process of risk assessment of data. See Section (6) (A) (7) of this Guideline for more on Data Categorization. See also "High Risk Data" and "Low Risk Data."

High Risk Data means data, the loss of confidentiality, integrity or availability of which could be expected to have a severe or catastrophic adverse effect on State operations, State assets, or individuals. High Risk Data includes Confidential Information as defined in in Bulletin 3.5.

Information Technology (IT) Activities include (A) the creation, collection, processing, storage, management, transmission, or conversion of electronic data, documents, or

records; and (B) the design, construction, purchase, installation, maintenance, or operation of systems, including hardware, software, and services which performed, or are contracted under Bulletin 3.5 to perform, these activities (see 3 V.S.A. § 2222(a)(10)).

Infrastructure as a Service (IaaS) means the remote infrastructure provided by a third party required for data processing, storage, networks, and other fundamental computing resources where the State is able to deploy and run arbitrary software, including operating systems and applications. The State does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability.

Integrity means guarding against improper modification or destruction of data, and includes ensuring non-repudiation and authenticity of State Data. Non-repudiation is the ability to prove an event has taken place so it cannot be repudiated later. For example, non-repudiation for an email is used to guarantee a recipient cannot deny receiving a message and the sender cannot deny sending it.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and the rights, title, and interest a person may have in them.

Low Risk Data means data, the loss of confidentiality, integrity or availability of which could be expected to have a **limited** adverse effect on State operations, State assets, or individuals. Low Risk Data includes all State Data which is generally available to the public. Low risk data cannot include any data that is confidential by law.

Platform as a Service (PaaS) is defined as the capability provided to the consumer to deploy onto the cloud infrastructure State- created or -acquired software applications created using programming languages and tools supported by the PaaS provider. The State

does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed software applications and possibly software application hosting environment configurations.

Product means any Commodity or service (as defined in Bulletin 3.5) which may include web-based subscription services and certain SaaS, PaaS and IaaS.

Security Breach means the unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of a consumer's Confidential Information.

Security Objectives refers to the three security objectives for data and State information technology activities: Confidentiality, Integrity, and Availability.

Service Level Agreement (SLA) means the vendor's service level commitments incorporated into a contract. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) means a web-based software application running on non-State infrastructure (commonly referred to as "cloud" infrastructure). The State does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual software application capabilities, with the possible exception of limited user-specific application configuration settings.

State Data means all information, whether in oral or written (including electronic) form created by or in any way originating with the State, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by, or in any way originating with, the State in the course of using and configuring the Services provided under a contract. Examples of State data include, but are not limited to, video streams, recorded phone conversations, logged text messages as well as database contents.

4. Roles and Responsibilities in IT Procurement

Before undertaking an IT procurement, it is important to understand the respective roles of the contracting Agency, Department of Information and Innovation ("DII"), the Office of Purchasing & Contracting ("OPC") and the Office of the Attorney General ("AGO"), as they relate to IT projects. The contracting Agency, OPC, DII the AGO and will work collaboratively during the IT Activity procurement and contract life cycle.

A. Contracting Agency

Each contracting Agency shall do the research and planning required to determine the appropriate IT Products or services for the Agency's needs. The contracting Agency must (i) communicate with OPC about the appropriate procurement options for the Products or services desired, contractor solicitation and contractor selection; (ii) communicate with DII to address DII administrative, project management, project oversight, desired business outcomes and other requirements; and (iii) communicate with the AGO about business needs, appropriate contract terms and whether AGO assistance with contract negotiations is desired. The contracting Agency will be responsible for reviewing prospective vendor alternatives and making a selection; this may involve the issuance of an RFP and committing the time and resources to a vendor selection process. Once a vendor has been selected, the contracting Agency will be essential to the contract negotiation process. Finally, once a contract has been executed, a contracting Agency will be responsible for appropriate contract management and ensuring compliance with contract terms.

All of this is covered in greater detail below in Sections **5(a) Hardware and Software, 6 IT Procurement and Planning – How to Get Started, 7 Procurement and Selection Process and 9 Contract Negotiations. Please note, contract approval processes are covered in Bulletin 3.5.**

B. DII

DII is responsible, under 22 V.S.A. § 901(a)(1), for providing direction and oversight for all activities directly related to information technology and information security, including telecommunications services, information technology equipment, software, accessibility, and networks in State government.

State Chief Information Officer (CIO) approval is required for:

- **A Business Case** (called the IT ABC form): approval is required prior to RFP or contract approval for IT activities with estimated lifecycle costs exceeding $500,000. See Section A.5 for more information.
- **Requests for Proposals** (RFPs) for information technology (IT) and information security, regardless of the dollar value;
- **Contracts** for information technology and information security as set forth under section X.B.4 of Bulletin 3.5.

RFPs and contracts are reviewed within DII prior to being submitted for CIO approval. DII's review is facilitated by the IT Procurement & Contracting group and consists of reviewers from the following DII divisions:

- **IT Procurement & Contracting:** Reviews for clarity and to ensure an appropriate IT RFP or IT Contract template was used and completely populated. Determines if the estimated lifecycle costs are over $500,000. If so, checks with the Enterprise Project Management Office (EPMO) for a CIO-approved IT ABC Form. If needed, advises the Agency to complete and approve the IT ABC Form prior to State CIO contract approval.
  IT Procurement & Contracting acts as the clearinghouse for RFPs, IT ABC Forms, and contracts requiring signature by the State CIO. In such cases, IT Procurement & Contracting must receive documents for review at least two weeks before the planned execution date. If less time is available, a letter of explanation should be attached. IT Procurement & Contracting obtains the necessary approvals within DII prior to sending to the State CIO for final approval.

A DII Review Verification Sheet (new as of 7/1/2016) that verifies that the contract was reviewed by DII Security, Enterprise Architect, and Enterprise Project Management Office. DII IT Contracting & Procurement group will provide the Agency with this sheet upon completion of this DII review which should be performed prior to routing a contract package. The State CIO will not approve contracts that don't include this sheet.

- **Security:** Agencies shall ask for security consultation early in the RFP process in order to ensure appropriate protection of the State's data. Validates that the RFP or contract includes appropriate security requirements, with reference to applicable State and federal laws, regulations, rules, policies and standards. These are determined based Data Categorization (see Section (6) (A) (7), Data Categorization).

- **Enterprise Architecture (EA):** Agencies should ask for EA consultation early in RFP development. The EA can provide insight into potential services already in use within the State that may be leveraged to achieve better value for the State. They can also help Agencies understand what business capabilities and processes will be effected by the new Product or service being sought.

  When reviewing RFPs and contracts, the EA is looking for alignment between the business needs and the technology being pursued; that the appropriate non-functional/technical requirements (e.g. for architecture, hosting, service levels, etc.) are included; and that relevant State and federal laws, regulations, rules, policies and standards are referenced.

- **EPMO**: Review is only performed for IT activities with estimated lifecycle costs over $500,000 which require project management. EPMO's focus is to ensure the RFPs and contracts include appropriate project management deliverables, functions, and qualifications.

DII is also responsible for obtaining independent review of any recommendation for an IT Activity, when its total cost is $ 1,000,000.00 or greater or when required by the State Chief Information Officer (see Section7, Independent Review).

C. OFFICE OF PURCHASING & CONTRACTING (OPC)

OPC is the central purchasing authority for IT Products and services. OPC has the expertise and staff to guide Agencies through the competitive procurement process. OPC responsibility includes overseeing the bidding and contracting process to ensure compliance with Bulletin 3.5, this Guideline and relevant State statutes and Executive Orders. OPC is also responsible for posting on-line all IT Activity RFIs, RFCs, RFPs and Requests for Quote (RFQ) regardless of type and cost. IT procurement forms, including templates for RFPs and IT contracts can be found on-line at http://bgs.vermont.gov/purchasing-contracting/forms.

D. OFFICE OF THE ATTORNEY GENERAL

The Office of the Attorney General (AGO) has the expertise to provide assistance with RFP development, complex contract negotiations and contract interpretation. The AGO is required by law to review all contracts over $25,000 for compliance with 3 VSA § 342. Additionally, Bulletin 3.5 requires the AGO to approve all contracts over $25,000 "as to form" (see Bulletin 3.5 Section X(B)(1)). IT contracting often involves issues of liability and risk management; data ownership, access to data, security and audit requirements, privacy and Confidentiality; data breach and breach notification; and intellectual property ownership. Further, IT contracts will very commonly involve the use of "small print" vendor forms, including licenses and other user agreements which raise these and other legal issues. The AGO has prepared a Standard Rider to Software and End User License Agreements ("Standard State Rider"), to be used with software commodity purchases and "as-is" web-based SaaS, PaaS and IaaS as discussed in greater detail below in **Section 5, Types of Information Technology Procurements**. The AGO has also prepared suggested terms for IT Professional Services and IT System Implementation Services. Current versions of "Attachment D" IT terms are available online at: http://bgs.vermont.gov/purchasing-contracting/forms, and are intended as a starting point for thinking through and addressing issues common to IT services. Agencies are expected to tailor the provisions to meet the requirements as appropriate for the type and scope of services involved. Finally, not every IT project implementation will proceed as expected. The AGO can advise client Agencies on contract terms, including payment terms, which appropriately address issues around non-performance or inadequate performance. Many of these issues can and should be addressed at the RFP stage, as discussed below in **Section 7(e), Procurement and Selection Process, Request for Proposal.**

5. TYPES OF INFORMATION TECHNOLOGY PROCUREMENTS

A. Introduction

Agencies may procure various types of IT products and services as described in greater detail below, including:

- Software only, hardware only or software and hardware which may or may not require related vendor services, such as installation, configuration, maintenance and support (all of which may be commodities contracts under the purview of OPC and subject to the processes in place for procuring Products) see existing Statewide Contracts at http://bgs.vermont.gov/purchasing-contracting/contract-info/current ;
- Acquisition of a complete system to be hosted on internal State servers (including software and possibly hardware) significant vendor services, such as installation, implementation, configuration, data conversion, training, deployment, support and maintenance see IT Procurement Planning at (6) (A);
- Service only (SaaS, PaaS and IaaS) which are subscription based services that may or may not require configuration from the vendor but do require ongoing maintenance and support;
- Consulting and other professional services, such as project consulting, project management, independent verification and validation (IVV), independent review (IR) and business analyst services, see IT Retainer Contracts at http://dii.vermont.gov/consulting/procurement/retainer ; and
- Security services such as Penetration (Pen) Testing Services and data security analysis which could include a vulnerability assessment through system and software testing or network security scanning, and services designed to assess business function, where threats come from, and agency security goals see IT Retainer Contracts at http://dii.vermont.gov/consulting/procurement/retainer.

B. Hardware and Software – Commodity Purchases

Often an Agency will need to purchase equipment or software. Hardware includes tangible equipment, such as computers, laptops, tablets, information processing units, servers, network

facilities, controllers, routers, firewalls, modems, communications and telecommunications equipment (voice, data, audio and video), cables, storage devices and media, printers, terminals, peripherals, input, output and transmission devices, and other tangible fixtures, mechanical and electronic equipment.

Software can include (i) operating system software, such as Windows which enables a user to interact with the hardware, and (ii) application software which provides certain desired functionality. The State acquires its software most commonly through third party resellers who are not the actual licensor (publisher) of the software. When an Agency acquires software, the software will always be licensed from the publisher through a license or user agreement.

All software, web-based subscription services, SaaS, PaaS and IaaS and certain hardware which incorporates software will be delivered subject to license and other user agreements which must be reviewed by the AGO and will likely require the attachment of a Standard State Rider, the template for which can be found on the OPC website at http://bgs.vermont.gov/purchasing-contracting/forms. **Note:** If purchasing software from an OPC contracted reseller please be aware contracted resellers are obligated by the contract to provide the Contracting Agency copies of all applicable license and/or or user agreements at time of quote.

(1) Getting Started with Hardware, Software and other Subscription Purchases

The OPC is responsible for coordinating software and hardware purchases for the State. General steps for that process are:

STEP #1: Contracting Agency Determines Need. The contracting Agency must define need, when the Product is needed, and any special requirements, such as data security specifications.

STEP #2: Can a Statewide Contract Satisfy the Business Need? The contracting Agency can determine if a Statewide Contract exists that meets its needs by contacting the OPC or referring to list of Statewide Contracts maintained at http://bgs.vermont.gov/purchasing.

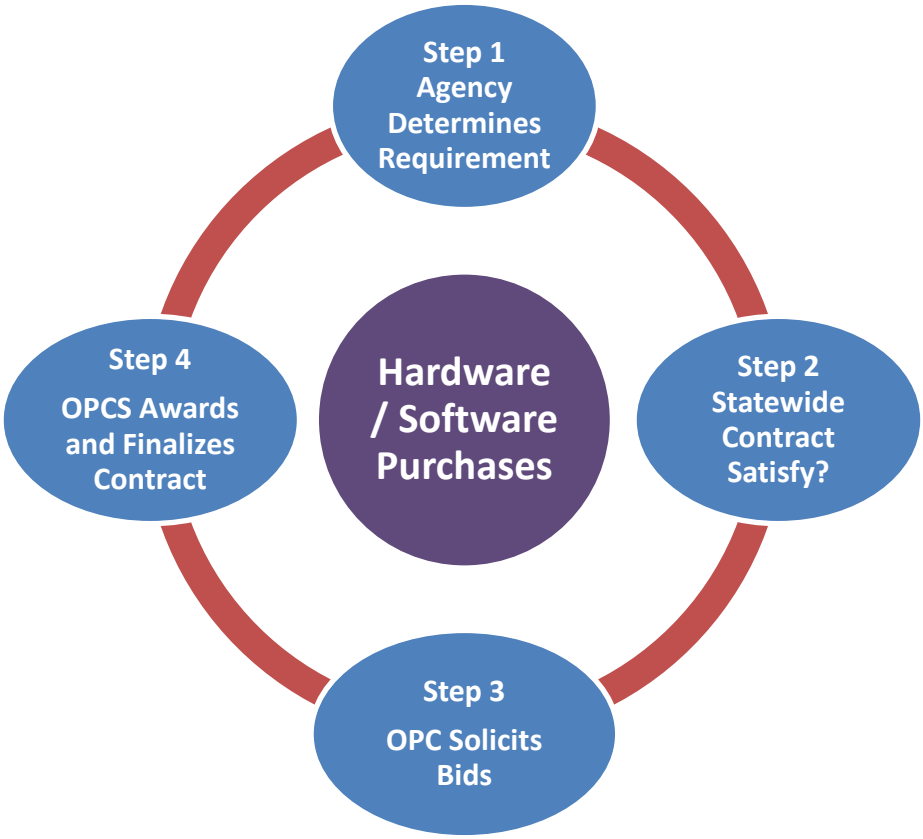
- YES! Follow Agency procedures for purchasing under Statewide Contracts. Purchases under Statewide Contracts must be made in accordance with the Contract's "Method of Ordering" instructions. This is a critical step in the process. These Statewide Contracts were established in concert with DII and the AGO and include the steps and tools

(documentation) necessary with respect to purchase considerations such as cost thresholds, responsibilities, approval gates, confidentiality, security and legal liability. As always, a Contracting Agency may contact the OPC with any questions.

- NO! Go to Step 3.

STEP #3: OPC Solicits Bids. If a Contracting Agency's need cannot be met via an existing Statewide Contract, the Contracting Agency will work in consultation with the OPC to determine the appropriate means for soliciting bids (i.e., whether a detailed RFP or RFQ might be required). OPC will assume primary responsibility for administering the solicitation process. During this step in the process, a Contracting Agency will provide necessary subject matter expertise and can expect to assist OPC in reviewing bids for technical compliance.

STEP #4: OPC Awards and Finalizes Contract. Once an award is made, the Contracting Agency may need to provide business input during negotiation and contracting. Licenses and other user agreements must be reviewed by the AGO and will likely require the attachment of a Standard State Rider, the template for which can be found on the OPC website at http://bgs.vermont.gov/purchasing-contracting/forms



C. System Acquisition

Many IT Activities will involve the acquisition of a complete system to be hosted on State servers (including software, possibly hardware and remote maintenance and support services) or SaaS, PaaS or IaaS located off-site on a vendor's servers or "cloud." These system acquisitions will require significant vendor professional services, including project management, installation, implementation, configuration, data conversion and migration, training, deployment, support and maintenance as well as licensing and end-user licensing considerations. These projects will require an Agency to establish a governance structure, including identification of a project sponsor, a business lead and an in-house or contracted project manager (who may be the same as the business lead), as described below in Section 6(A), IT Procurement Lifecycle, IT Procurement Planning. These IT activities will require substantial planning and must involve a solicitation, selection and contracting process. These steps are covered below in **Section 7, Procurement and Selection Process.**

D. Consulting and other Professional Services

Agencies may consider IT consulting services for numerous purposes such as:

- IT management consulting for assistance with developing long range IT plans and strategic planning;
- Project management for coordination and scheduling or project activities, assessing project requirements and facilitating project implementation and vendor management; and
- Business analysis which may be necessary to ensure IT activities successfully meet business and contract objectives;

Other IT services Agencies may require include content management, database administration, infrastructure support, LAN and server services, software services (including system integration and maintenance and support), systems engineering, security services and web design services.

These consulting and other professional services may be procured through a simplified OPC Retainer Agreement process if they are anticipated to be $100,000 or less (see Section X1 D3 1, IT Retainer Contracts). For any of these services which are anticipated to cost more than $100,000, Agencies must issue a Request for Proposal in accordance with Section VIII(B) of Bulletin 3.5.

E. Security

Agencies may seek services to develop strategies and solutions to defend hardware and software IT and telecommunications resources against adversaries such as viruses, worms and hackers for operating systems and applications, conduct penetration and other system vulnerability testing and perform related IT security activities. These activities must be coordinated with DII Security. See the DII website at http://dii.vermont.gov/consulting/procurement/retainer/security for examples of potential IT security scopes of work.

These IT security services may be procured through a simplified OPC Retainer Agreement process if they are anticipated to be $100,000 or less (see Section X1 D3 1, IT Retainer Contracts). For any of these services which are anticipated to cost more than $100,000, Agencies must issue a Request for Proposal in accordance with Section VIII(B) of Bulletin 3.5.

6. IT Procurement Lifecycle

The IT Procurement Lifecycle consists of the following stages:

1. **IT Procurement Planning:** Identify the contracting team and the project objectives and strategy, develop requirements and prepare a business case and cost analysis.
2. **IT Procurement and Selection:** Conduct the appropriate procurement and selection process; fairly and objectively select the contractor(s) that best meet the needs of the State in terms of cost and solutions.
3. **IT Contract Negotiation and Signing:** Ensure the contract contains provisions that hold the contractor accountable for producing the desired results and adhering to all terms and conditions.
4. **IT Vendor Management:** Monitor and enforce the terms of the contract.
5. **IT Vendor Decommissioning**

A. IT Procurement Planning – Stage 1

IT Procurement Planning is critical to the successful outcome of any procurement. With proper planning, State entities are more likely to successfully achieve their contracting objectives.

Procurement planning includes:

1. High Level Planning Meeting:

Depending on the size, scope, and complexity of a project, at the outset of an IT Activity, a Contracting Agency should convene a high level planning meeting to bring together key Agency staff to consult with the OPC, DII and the AGO in order to discuss the proposed project and Agency priorities, roles and responsibilities, possible procurement and contracting approaches, timeframe, Data Categorization and questions and concerns which may arise. A high level planning meeting is strongly encouraged for complex projects.

2. Identify those Individuals with Key Project Roles:

At a minimum, an Agency planning for an IT activity should identify:

a. Project Sponsor, who will act as the primary decision maker, marshal resources as needed, and ensure funding is available;
b. Business Lead who is the primary contact from the business area sponsoring the initiative, such as a Deputy Commissioner or Director from the business area;
c. Technical Lead who is the primary contact for technical and security issues and information. Agencies should consider using an enterprise architect from DII if there is no one with sufficient technical expertise in the Agency; and.
d. Project Manager (PM) who leads and manages the project. The PM may be the Business Lead or a contracted PM. See the EPMO website at http://epmo.vermont.gov/ for project roles and responsibilities.

In addition, an Agency should identify the representatives at OPC, AGO and DII who will assist with the planning, procurement, contracting and vendor management processes.

3. Determine Funding:

Determine a funding source and amount for the IT Activity (i.e., how much is the Agency prepared to spend and where will these funds come from?). It may be premature to start a procurement process if the Agency does not have answers to these funding questions.

4. Determining Potential Solutions and Estimated Costs:

An Agency must be prepared to propose a solution and provide estimated costs in order to prepare the Business Case/Cost Analysis (referred to as an "IT ABC form") (see Subsection 5 below "*Complete a Business Case & Cost Analysis (IT ABC form).* There are several ways to determine what kind of IT solutions might be available which would suit the needs of the Contracting Agency, such as:

- Checking with other states and/or industry contacts to find out what solutions they have employed and their estimated costs.
- Determining how other Vermont State agencies/departments are meeting similar business needs by consulting DII.
- Use the Request for Information (RFI) process to find out what products/solutions are available in the marketplace and to obtain cost estimates. See Bulletin 3.5, Section VI (B) (3) on the RFI process.
- Consult with DII's Enterprise Architecture group for information and solution suggestions.

5. Determine the requirements for the eventual decommissioning of the service

- Consult with DII Security to determine the requirements for retaining State ownership of data.
- Consult with DII Security to determine any additional requirements for ensuring the return and/or destruction of State data.

6. Complete IT ABC Form:

A contracting Agency should complete a business case and cost analysis (IT ABC Form) for the proposed IT Activity. CIO approval of the IT ABC form prior to procurement is required if the lifecycle costs of the IT Activity are expected to exceed $500,000. The IT ABC form is an important tool for substantiating the benefits of an IT Activity and for providing the justification for the investment of State dollars and labor. The IT ABC Form and IT ABC Form Instructions can be obtained from DII upon request or found online at http://epmo.vermont.gov/sites/epmo/files/Templates/PM/IT_ABC_Form.pdf . The Business Lead (or Project Manager if already assigned) must email the completed IT ABC form for projects anticipated to cost over $500,000 to DII.EPMO@vermont.gov . Upon receipt, the EPMO will assign an **Oversight Project Manager (OPM)** to facilitate the review and approval process.

7. Data Categorization:

Prior to any information technology procurement undertaking, an Agency must categorize the affected State Data as High or Low Risk. Data Security categories are based on the potential impact on the State should a Security Breach occur which jeopardizes the State Data and State IT Activities needed by the Agency to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. Data Categorization must be done on a case-by-case basis within the context of each procurement and the best interests of the State. DII Security and the AGO should be consulted to determine which laws, if any, apply to the protection of the affected State Data.

Considerations must be given to how the data will be used or accessed by the Contractor and whether it will involve the electronic processing, storing, or transmission of confidential or legally protected information. Additionally, consideration must be given to ownership of the data, and return or destruction of the data. Data categorization informs and enables the determination of the data security provisions that will be required by the State in the resulting agreement. It is important to note the above data security concerns exist whether the State is engaging in data use/sharing pursuant to a Contract or a Grant. Accordingly, an Agency must categorize the affected State Data prior to entering into any data use/sharing agreement, and ensure that the agreement includes appropriate requirements to protect the interests of the State.

8. Gather and document Functional and Technical (Non-Functional) Requirements:

Requirements describe the needed or desired capabilities of the product, solution, services and/or supplier, or performance requirements for deliverables, with reference to the applicable Data Categorization. Requirements provide a description and purpose of the IT Product or service needed but only include minimal functional specifications, usually including only those functions which correlate specifically with identified Agency business needs. Requirements should be compatible with existing equipment and should contain a description of the existing equipment along with any upgrade requirements or future needs.

It is important to clearly define all requirements prior to procurement for inclusion in the RFP and the subsequent contract. This step may take some time and resources to complete. Effective IT requirements will be written with certain characteristics that include:

- Simple: Avoid unnecessary detail, but be complete enough to ensure that requirements will satisfy their intended purpose.
- Clear: Use terminology that is understandable to the Agency and vendors. Avoid legalese type language and industry jargon whenever possible. Include definitions of terms where needed to mitigate conflicting interpretations and to align with State-specific technology terms and definitions.
- Informative: Describe the Agency's desired state for the IT activity, to include usage and audience and any technical/functional needs/restrictions, workflows or data flows, interface with other applications/systems and architecture for legacy systems, platforms and operating systems.
- Accurate: Use units of measure or performance compatible with industry standards. All delivery and acceptance requirements should be clearly identified. Include all required State, federal and/or national technical, professional, industry standards, specifications and certifications, as needed.
- Flexible: Avoid inflexible specifications which prevent the acceptance of a proposal that could offer greater performance for fewer dollars. Use approximate values such as dimensions, weight, speed, etc. (whenever possible) if they will satisfy the intended purpose. If approximate dimensions are used, it should be within a 10% rule of thumb unless otherwise stated in the solicitation document.
- Measurable: Ensure that requirements identify mutually verifiable conditions under which a requirement has been successfully met.

9. Identifying the Procurement Team

Once the above steps have been completed, the PM identified in step 2 will work with DII, AG's Office and the OPC to ensure that the appropriate members of the procurement team are engaged. The procurement team will include the following:

- **PM** – The PM should already be assigned to the project and will lead the procurement process.
- **DII Procurement Analyst** – Facilitates the DII review process and approval of RFPs and contracts.
- **OPC Representative** – This person will act as a guide to answer questions about the procurement process and ensure Bulleting 3.5 is followed. They will also post the RFP, receive RFP responses, receive questions from the vendors and post responses, field questions from vendors on the status of the award, and notify bidders once a contract has been signed.
- **AG Representative –** Ensures that the RFP and contract contain any State required legal language and attachments. Acts as an advisor to the team throughout the procurement process on legal issues and considerations. Participates in the contract negotiation with the selected vendor as needed/requested.
- **Project Sponsor** – Responsible for approving/signing off on the RFP and contract. Also the primary person accountable for negotiation of the contract.
- **The Business Lead and/or other Subject Matter Experts** designated by the Business to work on drafting the RFP, drafting language for the contract, and/or participating in the negotiating of the contract.
- **EPMO Oversight Project Manager:** Responsible for providing project oversight and for ensuring the appropriate project management deliverables are included in the RFP and contract. Coordinates the Independent Review process (if applicable).
- **DII Enterprise Architect –** Provides feedback early in the RFP and contract development processes to ensure DII technology standards are incorporated where applicable.
- **DII Security Representative –** Participates only if the solution involves the use, transmission or storage of personal identifiable information (PII) or any data that is confidential by law. Provides feedback early in the RFP and contract development processes to ensure DII security standards are incorporated where applicable.

10. Defining a Procurement Communication Plan

Define a plan that will meet the communication needs of the participants as well as to keep key project stakeholders informed. For example, how will team members be kept in the loop on the status of procurement tasks, decisions, etc.? Will you communicate through email, regular meetings, meetings as needed, etc.

11. Preparing for Procurement

With input/assistance from the Procurement Team, the PM should do the following:

a. Define the Procurement Approach

Based on guidance from Bulletin 3.5 and/or the OPC determine the approach to procurement (e.g., RFI, retainer contract, simplified bid, RFP, etc.). See Section 5 for more information about the procurement types.

b. Create a List of Items and Professional Services you are looking to procure

c. Assess the Readiness of your Requirements

Is your definition of requirements mature enough to begin drafting an RFP?

d. Create a Draft Procurement Schedule

IT is helpful for an Agency to estimate the timing for a procurement, particularly if there are service, staffing, funding or other constraints. A sample draft procurement schedule template and tasks is included as Appendix 1 at the end of this document.

e. Identify any Procurement Constraints, Risks, and/or Dependencies

Such as with cost, time, scope or any legal issues that need to be considered as part of the procurement process.

f. Identify any obtain copies of relevant Procurement Templates, Attachments and Addendums

g. Identify the Criteria for Vendor Selection

Determine what criteria is most important and assign a percentage to each criteria selected. Examples include: cost, experience of vendor staff, ability to meet all requirements, number of years in business, ability to meet proposed time line, customer service ratings, ability to meet on-going maintenance and support needs, etc.

h. *Determine the approach to writing the RFP*

Who will write it, who will review it, what is each reviewer covering, etc. Ensure that you have the most recent versions of all forms, which are available online at:

http://bgs.vermont.gov/purchasing-contracting/forms

i. *Determine a format for the vendor responses*

You can simplify your evaluation process if you define and require a standard format for your responses. This can help shorten the responses and make it easier to compare one proposal to another.

B. IT Procurement and Selection Process – Stage 2

Sections VII and VIII of Bulletin 3.5 describe competitive bidding thresholds and the various bidding processes. For IT contracting, as with most State contracting, an Agency should first contact the OPC to discuss the most appropriate procurement process for the Product or IT activity under consideration.

1. Statewide Contracts

Agencies should first confirm whether their business needs can be met through one or a combination of existing Statewide Contracts for IT Products and related services. See the description above in Section 5(B)(1). Statewide contracts are available on-line at: http://bgs.vermont.gov/purchasing-contracting/contract-info/current and specific technology contracts are available at: http://bgs.vermont.gov/content/communications-contracts . The process for utilizing Statewide Contracts can be found in Bulletin 3.5, Section XI (D)(1).

2. IT Retainer Contracts

The State has entered into a number of statewide Retainer Contracts with vendors to enable Agencies to quickly and efficiently obtain a variety of IT professional services. Vendors with Retainer Contracts provide services across various functional areas or categories of IT services a complete list of which can be found on the DII website at http://dii.vermont.gov/consulting/procurement/retainer. These range from IT strategy, planning and business analysis services to IT security, digital content management and systems engineering. The value of a Contracting Agency's contract with a Retainer Contract vendor must be $100,000 or less. IT retainer vendors and the Master Retainer Agreement with each vendor can be viewed at http://dii.vermont.gov/consulting/procurement/retainer . Each Retainer Contract sets out a process by which an Agency may select a vendor on retainer through a Statement of Work ("SOW") RFP process. The Agency should then negotiate an SOW Agreement with the selected vendor. A form Retainer Contract, which includes templates for the SOW RFP and the SOW Agreement can be found at http://bgs.vermont.gov/purchasing-contracting/forms. The Contracting Agency may directly utilize these Master Agreements in accordance with the Form SOW RFP and Form SOW Agreement process. An overview of the Statement of Work Process is identified below however detailed information on process is identified in each Retainer Contract.

Statement of Work Process Overview:

A. When a Contracting Agency has a need for services in one or more of the categories, the Agency will prepare and deliver an SOW RFP to the pre-qualified vendors on the list.
B. Vendors will then submit proposals within the date and time established by the Agency.
C. Following proposal evaluation, in the best interest of the State, the Agency may enter into an SOW Agreement with the selected vendor.

D. The resultant SOW Agreement will be administered by the Agency. Agencies shall provide DII Procurement & Contracts and OPC with copies of all executed SOW Agreements by sending to sov.itcontractingandprocurement@vermont.gov and SOV.OPC@vermont.gov .

E. Projects over $100,000 require Standard Request for Proposals (RFPs). Any State project having an actual or anticipated cost greater than $100,000 may not be executed pursuant to this Master Agreement, and must instead undergo a formal RFP process.

Additional information for utilizing Retainer Contracts can be found in Bulletin 3.5, Section XI (D)(3). As of the date of this Guideline, **OPC on behalf of DII has conducted a new retainer vendor search and the new list of retainer vendors will be maintained on-line on the OPC website at** http://bgs.vermont.gov/purchasing-contracting/contract-info/current**. Agencies are responsible for determining vendor qualification as part of the SOW RFP process.**

3. Request for Information (RFI) and Request for Comment (RFC)

The RFI and the RFC are described in greater detail in Bulletin 3.5, Sections VIII(B)(3) and (4) respectively, and are valuable tools for purposes of acquiring sufficient information for developing and articulating requirements for an effective Simplified Bid or RFP and maximizing opportunity and value for the State. Contracting Agencies should contact the OPC for guidance and more information on how to use these tools.

4. Simplified Bid

If an IT Activity is not available through either a Statewide Contract or a Retainer Contract, and it is expected to have a value of $100,000 or less, Agencies may use a simplified bid process as described in Bulletin 3.5, Section VIII (A). When procuring Products, Agencies must work through OPC in accordance with the process outlined in Section 5(B)(1) above

5. Request for Proposal (RFP)

The formation and foundation of an effective contract starts with the drafting of the solicitation. A Request for Proposal (RFP) is generally used for the procurement of IT activities in situations where price is not the sole determining factor and the award will be based on a combination of cost and technical factors to be determined in the best interest of the State. A template for an IT RFP can

be found at http://bgs.vermont.gov/purchasing-contracting/forms . A general discussion of effective RFP drafting can be found in Bulletin 3.5, Section VIII(B).

As discussed above in Section 5, appropriate planning is essential for a successful IT Activity RFP. It is essential for a Contracting Agency to define its high level project requirements as discussed above in Section 5(c). The Contracting Agency should anticipate an RFP process timeline to meet the Agency's programmatic needs and effectively budget staff time as discussed above in Section 10 (d), **Create a Draft Procurement Schedule**.

Using the information gathered during the IT Procurement Planning process described above, an Agency should easily be able to draft an initial draft of an RFP using the Sample Information Technology RFP shell found at http://bgs.vermont.gov/purchasing-contracting/forms. The State should determine how vendor performance will be measured so that service level expectations can be included in the RFP and contract. Each Agency should determine the approach to writing the RFP, such as who will write it, who will review it and what is each reviewer is responsible for covering. Again, DII must approve all IT RFPs. Agencies should determine what criteria for vendor selection are most important and assign a percentage to each of the criteria selected. Examples include cost, experience of vendor staff, ability to meet State functional, technical and service level requirements, number of years in business, ability to meet proposed time line, customer service ratings and ability to meet the State's on-going maintenance and support needs.

Intellectual Property Ownership and Licensing 3 V.S.A. §346 allows the State to grant to Contractors the right to use or own intellectual property developed for the State, for the Contractor's commercial purposes.

When drafting the RFP, Agencies must give consideration to Intellectual Property Ownership and Licensing**.** IT software development presents unique intellectual property ownership and licensing considerations. This is primarily because the State's procurement of a vendor's software product does not equate to ownership of the product in the traditional sense. Rather, what the State obtains when it procures a software is the right to use a vendor's product (i.e. a license). Generally speaking, when the State licenses a vendor's commercial off the shelf ("COTS") software the vendor will own the Intellectual Property developed prior to the State engagement or developed during but

outside of the State engagement. The vendor may also have the right to use certain pre-existing third party software in order to deliver the services. When this is the case, the State will require a license to use the vendor's software or applicable third party software for the term of the contract. The State will have no rights in the vendor's Intellectual Property, other than the rights granted in the licenses.

It is essential that the Business Lead consult with counsel or the AGO and DII to determine whether the scope of the license granted by a vendor is sufficient for the State's business purposes.

"Work Product" produced as a result of the vendor's services may have certain ownership rights but may be limited to tangible output generated by the State's use of a system, such as reports, graphs, charts and modified State Data.

Contracting agencies must make business decisions about whether they require right, title and ownership in certain tangible or intangible Work Product. For example, the State may hire a vendor to write new source code and develop a software product for the State. In this case, the State will pay for and could elect to own both the tangible and intangible Intellectual Property which is created. State ownership gives the State the right to modify, sell and use the software for any legal purpose. The Contracting Agency could determine, as a business decision, to license this new product to the software developer and other third parties for their own business purposes. This ownership may involve taking steps to copyright or patent the new product and monitoring its use.

Alternatively, the Contracting Agency could determine to transfer ownership of the new software to the developer. If the State transfers ownership to the software developer, the State must receive appropriate compensation, which may include a fully paid, royalty free, perpetual, irrevocable license to use the new software for any and all State purposes.

The State should also consider terms in the contract designed, at a minimum, to recover the State's initial investment through license fees or payment terms as a result of any transfer of rights.

Contracting agencies should consult with counsel or the AGO to discuss the pros and cons of ownership versus licensing and the legal requirements in connection with each. Such terms must be reviewed by the AGO and approved by the Secretary of Administration.

The State should also consider terms in the contract designed, at a minimum, to recover the State's initial investment through license fees or payment terms as a result of any transfer of rights.

Contracting agencies should consult with counsel or the AGO to discuss the pros and cons of ownership versus licensing and the legal requirements in connection with each. Such terms must be reviewed by the AGO and approved by the Secretary of Administration.

Once the RFP is issued, the Agency must determine how it will conduct the evaluation process, including who will review and score proposals, whether this will be done as a group activity or independently, what format/template will be used to document scores and the time period the Agency will schedule for RFP review.

As always, Agencies should feel free to consult with the OPC, DII and the AGO for advice and suggestions on RFP drafting. The RFP should be submitted to the Project Sponsor for review and approval. All Information Security and Information Technology RFPs must be reviewed by the CIO or her/his designee prior to posting. **Please allow for at least 2 weeks for the initial review and approval process.** Finally, RFPs that result in federally funded contracts may be subject to federal approval. Contracting Agencies are responsible for determining federal approval requirements.

IT Activities typically involve licensing, end user or other standard vendor terms and conditions. All vendor contract terms must be requested during the procurement process. All contract terms, including Contractor licensing, maintenance and support and service level terms, as applicable, shall be included in a single final State contract. Many vendor agreements typically appear on-line as an electronic "click through" agreement (such as "I Accept" or "I Agree"). All vendor terms must be provided to the State in hard copy and must be negotiated as a part of the final State contract.

All RFPs for IT Activities are to be sent to the OPC for posting in accordance with Bulletin 3.5, Section VI(B)(5). If applicable, Agencies should compile a list of any specific vendors to be notified of the specific solicitation and provide OPC with a contact name, company name and email address for each.

6. Vendor Selection

Once bids are submitted, Agencies should follow Bulletin 3.5, Section VIII (B) (8) on Contractor Selection and Documentation. If a Contracting Agency is seeking an off-the shelf software product or a web-based Software as a Service, the Contracting Agency should require demonstrations with all key Agency subject matter experts present as part of its selection process in order to test actual product functionality. **It is important to contact customer references.**

Selections must be made in accordance with any criteria specified in the RFP.

In order to avoid surprises during contract negotiations, it is advisable to have agency counsel or the AGO review vendor documents and vendor exceptions taken to Standard State terms. This may lead to discussions with potential vendors to determine the feasibility of moving forward with a selection.

7. Independent Review (if total lifecycle costs are over $1,000,000.00)

An Independent Review (IR) is required by law for IT Activities with a lifecycle cost of $1,000,000 or more, or at the discretion of the Commissioner of DII. An IR provides an independent assessment of a technology project, proposed solution, proposed vendor, and all the associated lifecycle costs (i.e., implementation and on-going operations). DII contracts for the IR; all IRs must include:

- Acquisition Cost Assessment
- Technology Architecture Review
- Implementation Plan Assessment (which includes a Risk Assessment)
- Cost Benefit Analysis
- Impact Analysis on Net Operating Costs for the agency carrying out the IT Activity; and
- Procurement Negotiation Advisory Services.

The IR contractor should be selected by DII prior to vendor selection so that the IR can be scheduled once a vendor is selected. Contract negotiations can begin while the IR is underway, but

a contract should not be executed until the IR is complete. Once the IR is complete, the Commissioner may either approve the project, requests additional information, request follow-up action prior to granting approval, or decline the project. Detailed information regarding preparation for an IR can be found on the EPMO website. See also the Draft Procurement Schedule found in Appendix 1 at the end of this document in order to estimate how the timing of the IR may affect the project implementation.

The cost of the IR is paid by the Contracting Agency. The cost for a standard IR cannot exceed $25,000. An IR with an expanded scope cannot exceed $50,000. The OPM (in conjunction with the Agency) defines the scope of the IR. Examples of an expanded scope include an IR that covers multiple projects and/or vendors.

A standard IR takes 5 to 6 weeks to complete. An IR with an expanded scope can take 8 weeks.

8. IT Contract Negotiation & Signing – Stage 3

Simultaneously with the IR process, Agencies should initiate contract drafting and negotiations with the selected vendor(s). Agencies must prepare a draft contract using the IT contract template found at http://bgs.vermont.gov/purchasing-contracting/forms. The template is a flexible tool and walks the drafter through the drafting process step-by-step. Provisions which are not applicable or not required from a business perspective may be deleted. Agency-specific project needs should be included. Representatives from the OPC, AGO and DII are available for consultation and assistance with drafting on legal, business and technical terms.

The projects with the best chance of success are negotiated with the active interest and involvement of the Project Sponsor, Business Lead, Project Manager and technical and legal resources. These members of the project team must be familiar with the vendor and the product selected, including the strengths and weaknesses of both vendor and product. These members of the project team will be called upon to make a variety of business decisions regarding scope and risk tolerance. Representatives from DII, OPC and the AGO can help contracting Agencies with methods and strategies for negotiating an IT contract and advise on (i) risks to avoid and (ii) proven methods for reaching agreement that will support a successful relationship and mutual project success.

1. Key points:

a. The more work an Agency has done at the outset to prepare for the procurement, the easier contract drafting and negotiations will be.

b. An effective negotiation team including the Project Sponsor, Business Lead, Project Manager and technical and legal resources is thoroughly prepared, has assigned roles and responsibilities and knows the technical and business requirements as well as the strengths and weaknesses of the State position versus those of the vendor.

c. In order to maintain the greatest negotiating leverage with a vendor, it is essential to have a "Plan B," which may include negotiating with second best bidder on a procurement, reissuance of the RFP or reevaluation of agency needs and timeframes.

d. To achieve the highest value from a contract negotiation, it is essential to go through a value engineering process that includes a prioritization of business requirements combined with a gap analysis of costs and vendor capabilities.

2. Considerations for IT Contract Terms and Conditions

The following Table describes some key contract considerations for when an Agency assembles a draft IT Contract. These proposed considerations do not address all issues an Agency may face, but are intended as a starting point.

ATTACHMENT A	
Attachment A	1. The Contract shall clearly identify the project purpose, objectives (desired outcomes and the process through which success can be measured) and Contractor expectations.
Attachment A	2. Contractor shall perform background checks acceptable to the State.

Attachment A	3. The State and the Contractor shall identify governance and project management structures consistent with this Bulletin and DII project management standards.
Attachment A	4. The State and Contractor shall specify contract staffing requirements and reserve the right of the State to request remove of key Contractor personnel.
Attachment A	5. Contractor shall comply with and adhere to the State IT Security Policy and Standards. These policies may be revised from time to time and the Contractor shall comply with all such revisions. Updated and revised versions of the State IT Security Policy and Standards are available at: http://dii.vermont.gov/policy/policy
Attachment A	6. As applicable, the State will provide requirements to Contractor for encryption of the data at rest or in transit.
Attachment A	7. System implementations shall include acceptance testing processes to be conducted by State subject matter experts before acceptance of all or any part of a new system.
Attachment A	8. Deliverable and project acceptance must be done in writing and shall not be given until the State has sufficient time to review and/or test, comment and accept or reject.
Attachment A	9. Final acceptance of and payment for a project should only be given once the State has confirmed the vendor has met all of the functional and technical requirements set out in the contract. Ideally a system will be required to function without material error for a period sufficient to address all potential business needs. The State should not agree to defer performance of "punch list" items into the warranty or support and maintenance phase.
Attachment A	10. The Master Contractor may deliver two copies of each software source code and software source code documentation to a State-approved escrow agent with the State's prior approval. The Master Contractor shall cause the escrow agent to place the software source code in the escrow agent's vaulted location. Two copies of the source code shall be stored on compact discs or other media designated by the State in a format acceptable to the State, and shall be easily readable and understandable by functional analysts and technical personnel with the skill set for that type of component, subcomponent, or software code.
Attachment A	11. Project functional and technical requirements from the RFP shall be set out in an Exhibit to Attachment A.

SaaS Specific Considerations	
Attachment A	12. The Contractor shall identify its hosting provider and subcontractor, if any, who will be involved in any application implementation and/or operations.
Attachment A	13. The contractor will ensure secure access to the application via a web interface (i.e. browser) across multiple devices to include desktop, laptop, tablet and other mobile devices. The contractor will be responsible for maintaining the software, upgrading it, and ensuring that it meets the states' requirements for confidentiality, integrity and availability consistent with the service level agreements specified in this document. The contractor will notify the state of pending version upgrades that may adversely impact our operations, prior to implementation.
Attachment A	14. The Contractor will be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Contractor. The environment and/or applications must be available on a 24 hours per day, 365 days per year basis.
Attachment A	15. The Contractor will ensure the State's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) are met (see Section (8) (3), Service Level Agreements).
Attachment B	
Attachment B	1. Contractor shall not submit an invoice until the State has delivered a written acceptance for the applicable deliverable.
Attachment B	2. For IT project implementations, the bulk of payments should be made only upon State acceptance of key functional deliverables. Agencies should either (i) back load payments, so the bulk of payments are made when the State is certain the product meets requirements and/or (ii) hold back a 15-25% retainage from each deliverable payment; the aggregate retainage is not paid until the State is certain the product meets requirements. Appropriately structured payment terms are one way to protect the State in the event of vendor non-performance.

Attachment B	3. Contractor invoices shall clearly differentiate any fixed costs for licensing, maintenance, support and/or hosting from costs for implementation services. To the extent vendor will not agree to costs are not invoiced and payable in arrears, the contract should require invoicing not less frequently than quarterly. .
Attachment D	
Attachment D	1. To the extent a Contractor Document, such as a license, end user agreement or other vendor terms and conditions, includes terms to which the State cannot agree, Attachment D should include superseding provisions.
Attachment D	2. The State shall own all right, title and interest in State data that is related to the services provided by the contract. As between the Contractor and the State, the State shall be deemed to be the owner of all customer data.
Attachment D	3. The State may seek to own or obtain a license to use all work (tangible and intangible intellectual property) produced by the Contractor in accordance with the contract, however any license to use must be broad enough for State purposes and as otherwise required by applicable law or regulations. If possible, the State should seek pricing concessions for work being transferred to the Contractor. (See Section 5 (a), Intellectual Property Licensing and Ownership)
Attachment D	Contractor shall procure and maintain (a) Technology Professional Liability insurance for any and all services performed under this Contract, with minimum third party coverage; and (b) first party Breach Notification Coverage in amounts acceptable to the Director of Risk Management. With respect to the first party Breach Notification Coverage, the State of Vermont and its officers and employees shall be included as additional insureds.
Attachment D	Limits of Liability (if any) Limits of liability, if any, agreed by the State shall be negotiated in consultation with in-house counsel or the AGO and shall be subject to the approval of the Director of Risk Management. All limits of liability shall exclude Contractor's obligation to indemnify the State, Contractor's confidentiality obligations to the State, personal injury or damage to real or personal property and Contractor's gross negligence, intentional misconduct or fraud.
Attachment D	4. Confidentiality and Security of High Risk State Data Protection of state data must be an integral part of the business activities of the Contractor to ensure there is no inappropriate use of

	State information at any time. To this end, the Contractor shall comply with the following conditions: High Risk Data processed, stored or accessible by the Contractor for any reason shall not be copied, disclosed, or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State. The Contractor may not use any High Risk Data processed, stored or accessible to Contractor in connection with the service provided under the contract for any purpose other than fulfilling the service. Contractor staff and subcontractors shall have access to data solely as required to perform job duties. State shall limit Contractor access, processing, storage or transmission of High Risk Data to solely the High Risk Data required for Contractor to provide the service. Contractor may be required to have employees undergo state background checks prior to handling High Risk Data.
Attachment D	5. The Contractor will make the State's Data and processes available to third parties only with the express written permission of the State.
Attachment D	6. The Contractor shall promptly notify the State of any request or demand for High Risk Data so the State may seek an appropriate protective order.
Attachment D	7. Contractor shall not store or transfer State Data outside of the continental United States.
Attachment D	8. Contractor must encrypt all High Risk Data in transit and at rest using FIPS 140-2 validated cryptography.
Attachment D	9. When High Risk Data is being accessed, processed, stored or transmitted, the Contractor will comply with National Institute of Standards and Technology (NIST) *Special Publication 800-53* (version 4 or higher) and *Federal Information Processing Standards Publication* 200 and (i) ensure the security and confidentiality of High Risk Data; (ii) protect against any anticipated security threats or hazards to the security or integrity of the High Risk Data; and (iii) protect against unauthorized access to or use of High Risk Data.
Attachment D	10. The Contractor will provide its Security Policy or other documentation of internal and external security controls, and its compliance level to NIST or other industry standards acceptable for the Data Categorization.
Attachment D	11. Security Breach

	When Contractor learns of an actual security breach or has a reasonable belief of an actual security breach that could compromise High Risk Data, the Contractor shall notify the State within 24 hours of its discovery and immediately determine the nature and extent of the Security Breach, contain the incident by stopping the unauthorized practice, recover records, shut down the system that was breached, revoke access and/or correct weaknesses in physical security. Full disclosure of the assets that might have been jeopardized must be made. In addition, the Contractor must inform the State of the actions it is taking or will take to reduce the risk of further loss to the State. Contractor shall analyze and document the incident and provide all notices required by the State.
Attachment D	12. The Contractor will cover the costs of response and recovery from a data breach and indemnify the State for all direct breach costs to the State.
Attachment D	13. Enhanced warranties The Contractor shall, at a minimum, warrant that (a) its system will comply with all applicable federal and State laws, regulations and rules; (b) will be free from material errors and shall perform in accordance with the specifications therefor; (c) the services shall be performed in a timely, diligent, professional and skillful manner, in accordance with the highest professional or technical standards applicable to such services, by qualified persons with the technical skills, training and experience to perform such services in the planned environment; and (d) any time software is delivered to the State, whether delivered via electronic media or the internet, no portion of such software or the media upon which it is stored or delivered will have any type of software routine or other element which is designed to facilitate unauthorized access to or intrusion upon, or unrequested disabling or erasure of, or unauthorized interference with the operation of any hardware, software, data or peripheral equipment of or utilized by the State.
Attachment D	14. When requested by the State, Contractor must destroy all requested State Data in all of its formats. High Risk Data shall be destroyed according to NIST SP 800-88R1 "*Guidelines for Media Sanitation*" and certificates of destruction must be provided to the State.
SaaS Specific Considerations	
Attachment D	15. The State must have the ability to import or export data in piecemeal or in its entirety at its discretion without interference from the Contractor in a format usable without the Service provided under the

	Contract and in an agreed-upon file format and medium at no additional cost to the State.
Attachment D	16. Upon the relocation of State Data, Contractor shall securely dispose of such copies from the former data location according to NIST SP 800-88R1 "*Guidelines for Media Sanitation*" and certify in writing to the State such State Data has been disposed of securely. Contractor shall comply with all reasonable directions provided by the State with respect to the disposal of State Data.
Attachment D	17. The Contractor shall run quarterly vulnerability assessments, promptly report results to the State and remediate all critical issues within 90 days, all medium issues within 120 days and low issues within 180 days.
Attachment D	18. The Contractor must allow the State to audit conformance to the contract terms and test for vulnerabilities. The State may perform this audit or contract with a third party to do so in its discretion.
Attachment D	19. The Contractor shall cause an SSAE 16 SOC 2 type 2 audit report or State-approved equivalent to be conducted annually.
Attachment D	20. The Contractor will provide evidence its Business Continuity Program is certified and mapped to the ISO 22301 standard.

3. Service Level Agreements.

A Service Level Agreement (SLA) is required for IT contracts when a vendor will be providing on-going maintenance and support services to the State. The SLA outlines the specific services and service delivery expectations. For example, a contract for a SaaS, IaaS or PaaS solution would include a description of the hosting services to be provided including availability, i.e. uptime expectations.

1. Key Topics to Cover in an SLA:

- Term covered by the SLA,
- Description of the services to be provided and their service levels (also called performance standards),
- The process, frequency and format for reporting on service levels,

- The remedies if the agreed upon services are not met (e.g., a credit on the next month's bill), and
- The process for review and changes to the SLA (including termination).

2. Defining your SLA starts with the RFP:

Identify your potential support and maintenance service needs for inclusion in your RFP. It's important that vendor bids include cost proposals for these services, and it's equally important to allow vendors to propose cost models for different levels of service (see defining services and service levels below). This allows you to see how your service requirements affect pricing. The details of your SLA are finalized in contract negotiations and will be included in your contract.

3. Defining Services and Service Levels:

The type of services included in a SLA will vary depending on the type of solution and your business needs. Below is a high level list of services for consideration for inclusion in your SLA:

- System Availability (uptime)
- System Performance (e.g., page load speed, transaction throughput, batch job timing, number of concurrent users, etc.)
- Customer Support (e.g., hours of support, response and resolution times, escalation process, etc.)
- Data Management (e.g. storage, retention, and back-up frequency)
- Disaster Recovery process including specifying a:
    - Recovery Point Objective (RPO: How much data can I afford to lose?)
    - Recovery Time Objective (RTO: How long can I go without service?)
- Security (e.g., data protection, access controls, security audits, confidentiality requirements, security breach identification and notification process, etc.)
- Hosted Services (e.g., access to data, location of data, accountabilities for third party service providers, etc.)
- Scheduled Maintenance/Downtime (notification and frequency)
- System/Software Upgrades and New Releases (e.g., frequency, documentation, bug fixes compatibility with custom code, etc.).

DII's Enterprise Architecture group can assist you in identifying your service level needs, as well as provide you with any applicable State and Federal standards that the SLA should adhere to.

4. Service and Service Level Examples:

<table>
<tr><th>Service</th><th colspan="3">Service Level / Performance Standard</th></tr>
<tr><td>Response Time</td><td colspan="3">95% of users will experience a response time of two seconds or less during regular working hours of 6:00 AM to 6:00 PM EST.</td></tr>
<tr><td>Throughput</td><td colspan="3">A file transfer/download of at least x mb (file size) will be transferred in x minutes.</td></tr>
<tr><td>Capacity</td><td colspan="3">System will support 800 concurrent internal and external users at peak time (6:00am - 6:00pm EST).</td></tr>
<tr><td rowspan="6">Customer Support</td><td colspan="3">Severity level is assigned by the State with the response and resolution times as follows:</td></tr>
<tr><td>Severity Level</td><td>Response Time</td><td>Resolution Time</td></tr>
<tr><td>1</td><td>15 minutes</td><td>30 minutes</td></tr>
<tr><td>2</td><td>30 minutes</td><td>4 hours</td></tr>
<tr><td>3</td><td>2 hours</td><td>48 hours</td></tr>
<tr><td>4</td><td>1 day</td><td>1 week</td></tr>
<tr><td>Availability</td><td colspan="3">The application will be available 99.9% of the time, 7 days a week, 24 hours a day and 365 days a year.</td></tr>
</table>

Plan of Action and Milestones (POA&M) Service Level Requirements

Commencement	Description	Data Sources	Service Level Metric
Upon acceptance as a vulnerability that has been ranked and entered onto the POA&M	Once a finding from a given assessment source has been identified as a vulnerability specifically assigned and the responsibility of Contractor, the vulnerability will be provided to (agency name) with a proposed ranking, milestones, point of contact and due dates. (Agency name) will confirm the ranking according to (governing) standards, approve the	Including, but not limited to, independent assessments, self-attestations, vulnerability assessments, pen test or incident/risk reports.	Resolution of: High ranked risks – 30 days Moderate ranked risks – 180 days Low ranked risks – 365 days

	risk content and the risk will be entered into the POA&M.		
Upon agreement of ownership of a POA&M assigned to the contractor	Once a finding has been mutually agreed as the Contractor's responsibility, Contractor will identify resources, provide a milestone description and target dates for completion of each milestone.	Including, but not limited to, independent assessments, self-attestations, vulnerability assessments, pen test or incident/risk reports.	Maintenance and Operations Staff will identify resources, provide a milestone description, and provide target completion dates for each milestone within 10 business days

Service Level Credit	0.25% reduction of the monthly fee for (Vendor Name) invoiced for the month in which a Service Level default occurred for each occurrence where a POA&M time requirement in the *Service level metric* was not met, with a maximum of up to the At-Risk amount.

5. SLA Dos and Don'ts:

- **Do** include your service level expectations in your vendor contract.
- **Do** keep the SLA simple, measurable and realistic. It is important to understand that SLAs cannot cover every possible situation that may arise.
- **Do** give the appropriate time and focus to outlining the SLA provisions in your contract. Often the primary focus in contract negotiations is the impending project and the SLA isn't given the same amount of scrutiny/consideration.
- **Don't** leave SLA details to be agreed upon at a later date. Reach agreement on the SLA provisions during contract negotiations (while you have bargaining power) and include those details in the contract.
- **Don't** ask for services or higher service level commitments than you actually need. This can drive up the cost of your project unnecessarily.

9. Vendor Management – Stage 4

Once the Contractor and the Agency have signed a contract for product(s) and services the parties are ready to begin the implementation portion of the IT Activity.

Vendor Management is about monitoring vendor performance to ensure the vendor is adhering to the Contract provisions. This monitoring takes place through project completion and continues for the term of the contract, which often includes on-going maintenance and support.

APPENDIX 1: Procurement Schedule Template and Tasks

Procurement Task	Responsible	Due Date
1. Determine Procurement Team	Agency PM	
2. Determine a Procurement Communication Plan	Agency PM	
3. Create List of Items and Services to Procure	Agency PM	
4. Assess Readiness of your Requirements	Agency PM	
5. Identify Procurement Constraints, Risks and Dependencies	Procurement Team	
6. Identify and obtain copies of the relevant Procurement Templates, Attachments and Addendums	Agency PM with help from OPC	
7. Identify the Criteria for Vendor Selection	Evaluation Team	
8. Determine the approach to writing the RFP	Agency Participants	
9. Define how you will conduct the proposal evaluation process	Evaluation Team	
10. Categorize the affected State Data as High or Low Risk	Agency PM with help from DII Security and AGO	
11. Determine how Vendor Performance will be measured	Agency Participants	
12. Determine Procurement documentation storage and organization	Agency PM	
13. Draft RFP	Agency Participants	
14. RFP Review	Agency, AG, & DII, & OPC	

15. Approve RFP	DII CIO	
16. Publish RFP	OPC	
17. Establish Deadline for Questions from potential Respondents	OPC and Agency PM	
18. Respond to Vendor Questions by the established deadline	Agency PM to coordinate may require input from DII, AG or OPC	
19. Establish RFP Deadline for Proposals	OPC and Agency PM	
20. Review & Evaluate Bids	Evaluation Team	
21. Evaluation Team meeting to determine finalists	Agency PM to schedule for Agency Participants	
22. Schedule demonstrations for finalists	OPC and Agency PM	
23. Perform Evaluations of Finalists	Evaluation Team	
24. Evaluation Team meeting to discuss revised scores based on the demos	Evaluation Team	
25. BAFOs requested	OPC in conjunction with Agency PM	
26. Perform Reference Checks	Evaluation Team designees	
27. Determine dates for the Independent review (IR) if applicable	DII OPM & Agency PM	
28. SOW is sent for IR if applicable	DII	
29. Evaluation Team Meeting for final selection	Agency PM	
30. IR Reviewer is selected and dates for the IR are finalized	DII OPM	
31. IR begins/ IR coordination	Agency PM & DII OPM	
32. Coordination of Contract negotiations	Agency PM	

33. Draft Contract	Agency participants	
34. Contract Review	Agency, AG & DII	
35. IR Meeting (Schedule & Facilitate)	DII OPM	
36. CIO approval is given for the project to proceed based on the IR report.	DII OPM coordinates obtaining CIO approval	
37. Coordinate Contract signing	Agency PM & DII Contracting	
38. Contract Award Notice published	OPC	
39. Coordinate Vendor's Start on the project	Agency PM	
40. Monitor Vendor Performance during the project	Agency PM or their designee	
41. Determine who will monitor vendor performance post-project for on-going maintenance & support if applicable.	Agency PM facilitates the discussion	