

**STATE OF MARYLAND
COMPTROLLER OF MARYLAND**

INVITATION FOR BIDS NO. 0802

FOR

**ACQUISITION OF
IBM TS3500 Tape Libraries and
TS7740 Virtual Tape System
FOR
THE ANNAPOLIS DATA CENTER**

ISSUING OFFICE

COMPTROLLER OF MARYLAND
ANNAPOLIS, MARYLAND
JOHN T. SALMON, PROCUREMENT OFFICER

ISSUE DATE

SEPTEMBER 20, 2007

Any prospective Bidder who has received this document from a source other than the Issuing Office should immediately contact the Procurement Officer via e-mail: ifb0802@comp.state.md.us and provide their name and mailing address in order that amendments to the IFB or other communications can be sent to them. Any prospective Bidder who fails to notify the Procurement Officer with this information assumes complete responsibility in the event that it does not receive communications from the Issuing Office prior to the closing date.

Minority business enterprises are encouraged to respond to this solicitation notice

Table of Contents

SECTION ONE -- GENERAL INFORMATION FOR BIDDERS

	IFB 0802 Summary Sheet.....	1
1.1	Overview	2
1.2	Description of Requirements	2
1.3	Abbreviations and Definitions	2
1.4	The Issuing Office	3
1.5	Contract Type.....	3
1.6	Term of Contract	3
1.7	Consideration and Payment.....	3
1.8	Pre-Bid Conference	4
1.9	eMaryland Marketplace	4
1.10	Questions.....	4
1.11	Bid Due (Closing) Date	5
1.12	Duration of Bid.....	5
1.13	Revisions to the IFB.....	5
1.14	Cancellation of the IFB; Rejection of all Bids	5
1.15	Procurement Method.....	5
1.16	Incurred Expenses	5
1.17	Bid Acceptance	5
1.18	Protests	6
1.19	Multiple Bids / Alternate Solutions	6
1.20	Access to Public Records Act Notice	6
1.21	Confidentiality.....	6
1.22	Bidder Responsibilities	6
1.23	Bid Affidavit and Contract Affidavit	6
1.24	Contract Agreement	7
1.25	Order of Precedence.....	7
1.26	Arrearages	7
1.27	Non-Visual Access	8
1.28	Basis for the Award of a Contract.....	8
1.29	Verification of Registration and Tax Payment	8
1.30	False Statements.....	8
1.31	MBE Participation Goal.....	9
1.32	Living Wage Requirement	9

SECTION TWO – BIDDER’S QUALIFICATIONS

2.0	Line of Business.....	10
------------	------------------------------	-----------

SECTION THREE – STATEMENT OF WORK

3.0	Hardware Requirements	11
3.1	Delivery Requirements	13
3.2	Cabling Requirements	13
3.3	Installation and Configuration Requirements	13
3.3.1	Hardware	13
3.3.2	Customization of z/OS Software and Migration Services	13
3.4	System Assurance and Implementation Planning	14
3.5	Performance Period of Acceptance	14
3.6	De-Installation and Removal of Replaced Hardware.....	14
3.7	Training Requirements	15
3.8	Documentation Requirements	15
3.9	Warranty and Maintenance.....	15
3.10	Security Requirements	15

SECTION FOUR – BID FORMAT

4.0	Bid Format	17
4.1	Bid Documentation	17
4.1.1	Transmittal Letter	17
4.1.2	Confidential Declarations.....	17
4.1.3	Management Summary	18
4.1.4	Bidder’s Affirmation of All Section Three Requirements	18
4.1.5	Bid Affidavit	18
4.1.6	MBE Utilization Forms	18
4.2	Bid Price Form	18

Appendices

Appendix A	Mandatory Contract Provisions	A
Appendix B	Bid Affidavit	B
Appendix C	Contract Affidavit.....	C
Appendix D	Bid Price Form	D
Appendix E	Sample Contract Agreement.....	E
Appendix F	MBE Utilization and Participation Forms	F
Appendix G	State of Maryland IT Security Policy.....	G
Appendix H	Vendor Electronic Funds Registration Request Form	H
Appendix I	Living Wage Requirements for Service Contracts	I

IFB 0802 SUMMARY SHEET

The Comptroller of Maryland is seeking to replace its IBM 3494 Automated Tape Library and 3494-B18 Virtual Tape System with an IBM TS3500 Automated Tape Library and IBM TS7740 Virtual Tape System.

NAME:	Tape Libraries and Virtual Tape System
ISSUE DATE:	September 20, 2007
Closing Date and Time:	October 18, 2007 at 5:00 pm
Issuing Office:	Comptroller of Maryland Information Technology Division Director's Office
Procurement Officer:	John T. Salmon Fax: (410) 974-2762 e-mail: ifb0802@comp.state.md.us
Pre-Bid Conference:	October 3, 2007 at 10:00 a.m. Annapolis Data Center 108 Carroll Street
Questions are to be sent via e-mail to: Questions must be submitted no later than 5:00 p.m., October 5, 2007.	Email Address: ifb0802@comp.state.md.us Attention: IFB0802-Tape System Question
Bids are to be sent via e-mail to: Bids must be submitted no later than 5:00 p.m., EDT, October 18, 2007	Email Address: ifb0802@comp.state.md.us Attention: IFB0802-Tape System Bid
IFB Number:	0802

**STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802**

**ACQUISITION OF
IBM TS3500 Tape Libraries and
TS7740 Virtual Tape System
FOR
THE ANNAPOLIS DATA CENTER**

SECTION ONE - GENERAL INFORMATION

1.1 OVERVIEW

The Comptroller of Maryland's Information Technology Division's Annapolis Data Center (ADC) provides mainframe computer services for nine (9) primary and fifteen (15) secondary user agencies.

The ADC central processing unit (CPU) is currently an IBM z890 Enterprise Server Model 2086-A04 with a capacity setting of 370 rated at 1,040 million instructions per second (MIPS), running the IBM z/OS operating system V.1.7.

1.2 DESCRIPTION OF REQUIREMENTS

The Comptroller of Maryland, through its Information Technology Division, is seeking to replace its IBM 3494 Automated Tape Library and 3494-B18 Virtual Tape System with an IBM TS3500 Automated Tape Library and IBM TS7740 Virtual Tape System in Annapolis and add a TS3500 Automated Tape Library in Baltimore that includes the purchase, installation, warranty and maintenance. No substitution equipment or alternate solutions may be bid in response to this solicitation.

1.3 ABBREVIATIONS AND DEFINITIONS

For the purposes of this IFB, the following abbreviations or terms have the meanings indicated below:

- a. ADC - Annapolis Data Center.
- b. Agency – The unit of State government procuring equipment and services.
- c. Agency point of contact – Person designated (Sect. 1.4) as the single point of contact for the Agency in this Invitation for Bids.

- d. Contract – The Contract attached to this IFB as Appendix E.
- e. Contractor – Winning bidder.
- f. COMAR – Code of Maryland Regulations.
- g. Comptroller – Comptroller of Maryland.
- h. Issuing Office – Comptroller of Maryland, Information Technology Division.
- i. Local Time – Time in the Eastern Time Zone as observed by the State.
- j. Bidder – An entity that submits an offer in response to this IFB.
- k. Procurement Officer – The State representative responsible for this IFB, for the determination of contract scope issues, and the only State representative that can authorize changes to the contract.
- l. IFB – Invitation for Bids.
- m. ITD - Information Technology Division.
- n. SOW – Statement of Work.
- o. State – Comptroller of Maryland and/or Agency.
- p. VTS - Virtual Tape System
- q. ATL - Automatic Tape Library
- r. OEM - Original equipment manufacturer

1.4 THE ISSUING OFFICE

The sole point of contact in the State for the purpose of this procurement is the Issuing Office.
The Issuing Office for IFB 0802 is as follows:

John T. Salmon, Procurement Officer
Comptroller of Maryland
Information Technology Division
Director's Office
Fax: (410) 974-2762
e-mail: ifb0802@comp.state.md.us

1.5 CONTRACT TYPE

This procurement is intended to provide a fixed price, not-to-exceed contract as governed by COMAR 21.06.03.02.

1.6 TERM OF CONTRACT

The contract resulting from this procurement will, upon approval by the appropriate agency authority, have a term of five years.

1.7 CONSIDERATION AND PAYMENT

By submitting a bid, the Bidder agrees to accept payments by electronic funds transfer unless the

Comptroller of Maryland grants an exemption. The winning Bidder shall register using the attached COT/GAD X10 Vendor Electronic Funds (EFT) Registration Request Form (Appendix H). Any request for exemption must be submitted to the Comptroller of Maryland for approval at the address specified on the COT/GAD X10 form and must include the business identification information as stated on the form and include the reason for the exemption.

1.8 PRE-BID CONFERENCE

A pre-bid conference will be held on **October 3, 2007**, beginning at **10:00 a.m.**, in Room 407A of the Annapolis Data Center Building, located at 108 Carroll Street, Annapolis, Maryland. While attendance at the pre-bid conference is not mandatory, information presented may be very informative; therefore, all interested vendors are encouraged to attend.

The conference will be transcribed. A copy of the transcript of the Pre-Bid Conference will be made available to potential Bidders at a nominal charge directly from the transcription company. The identity of the company and details of how to obtain a transcript copy will be provided at the conference. In addition, as promptly as is feasible subsequent to the Conference, a summary of the Pre-Bid Conference and all questions and answers known at that time will be distributed, via email, to all prospective Bidders known to have received a copy of this IFB.

In order to assure adequate seating and other accommodations at the Pre-Bid Conference, it is requested that all vendors planning to attend send an email to ifb0802@comp.state.md.us indicating their intentions by 3:00 PM on **October 2, 2007**.

In addition, if there is a need for sign language interpretation and/or other special accommodations due to a disability, it is requested that at least five days advance notice be provided. The Issuing Office will make reasonable efforts to provide such special accommodations.

1.9 eMARYLAND MARKETPLACE

In order to receive a contract award, Bidders must be registered on eMaryland Marketplace (registration is free). eMaryland Marketplace (<https://ebidmarketplace.com>) is an electronic commerce system administered by the Maryland Department of General Services. eMaryland Marketplace will be used, in addition to the Procurement Unit section of the Comptroller's web site (<http://compnet.comp.state.md.us/procurement>) and other means, for transmitting the IFB and associated materials, and providing answers to questions submitted by prospective Bidders, addenda, and other solicitation-related information.

1.10 QUESTIONS

Questions regarding the solicitation must be submitted in writing and transmitted by either email (IFB0802@comp.state.md.us) or fax (410) 974-2762. Questions must be received by **5:00 P.M., October 5, 2007**. A summary of all questions and answers will be distributed to all Bidders known to have received the IFB and will be posted on emarylandmarketplace.com and the Comptroller's web site (<http://compnet.comp.state.md.us/Procurement>).

1.11 BID DUE (CLOSING) DATE

Bidders must submit their bid package electronically as two separate files (may be zipped or unzipped) labeled in such a way as to identify which contains the Bidders Technical Documentation (example: BIDDERTNAMEifb0802techdoc.xxx) and which contains the Bidders Price Form (example: BIDDERTNAMEifb0802bidform.xxx). All files must be sent to: ifb0802@comp.state.md.us no later than 5:00 p.m., October 18, 2007. Bids arriving after the closing time and date will not be considered.

Requests for extension of this date or time will not be granted. Except as provided in COMAR 21.05.02.10, bids received by the Procurement Officer after the due date, October 18, 2007, at 5:00 PM (local time) will not be considered.

1.12 DURATION OF BID

The Bidder MUST state that its bid is valid for a period of a minimum of 120 days and may declare a longer period if desired. Such period may be extended by mutual written agreement.

1.13 REVISIONS TO THE IFB

If it becomes necessary to amend any part of the IFB or if additional data is necessary to enable the exact interpretation of provisions of this IFB, amendments will be provided to all Bidders who are known to have received a copy of the IFB. Acknowledgment of the receipt of all amendments will be required in the transmittal letter accompanying the Bidder's bid.

1.14 CANCELLATION OF THE IFB / REJECTION OF ALL BIDS

The State may cancel this IFB, in whole or in part, or may reject all bids submitted in response to this IFB whenever this action is determined to be fiscally advantageous to the State or otherwise in its best interests.

1.15 PROCUREMENT METHOD

This solicitation will be conducted in accordance with the rules governing procurement via multi-step competitive sealed bids as delineated in COMAR 21.05.02.17.

1.16 INCURRED EXPENSES

The State will not be responsible for any expenses incurred by a Bidder in preparing and submitting a bid. All bid submissions should be prepared simply and economically, providing a straight forward, concise delineation of the Bidder's capabilities to satisfy the requirements of this solicitation.

1.17 BID ACCEPTANCE

The State reserves the right to accept or reject any or all bids in whole or in part and to waive or permit cure of minor irregularities.

1.18 PROTESTS

A Bidder may protest the Notice of Intent to Award or the award of a contract as a result of this procurement. Any protest must be filed in accordance with Title 15, Subtitle 2 of the State Finance and Procurement Article, Annotated Code of Maryland, and COMAR Title 21 (State Procurement Regulations), Subtitle 10, Administrative and Civil Remedies.

1.19 MULTIPLE BIDS / ALTERNATE SOLUTIONS

Multiple bids and/or alternate solutions **will not** be accepted. An alternate solution is one that deviates from the stated mandatory requirements in this IFB.

1.20 ACCESS TO PUBLIC RECORDS ACT NOTICE

A Bidder should give specific attention to the identification of those portions, if any, of its submission that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Access to Public Records Act, State Government Article, Title 10, Subtitle 6, Annotated Code of Maryland. The ultimate determination of whether certain records or parts thereof are subject to disclosure rests with the procurement officer as custodian of the record.

1.21 CONFIDENTIALITY

Subject to the Maryland Public Information Act and any other applicable laws, all confidential or proprietary information and documentation relating to either party (including without limitation, any information or data stored within the Bidder's computer systems) shall be held in absolute confidence by the other party. Each party shall, however, be permitted to disclose relevant confidential information to its officers, agents and employees to the extent that such disclosure is necessary for the performance of their duties under this Contract, provided the data may be collected, used, disclosed, stored and disseminated only as provided by and consistent with the law. The provisions of this section shall not apply to information that (a) is lawfully in the public domain; (b) has been independently developed by the other party without violation of this Contract; (c) was already in the possession of such party, (d) was supplied to such party by a third party lawfully in possession thereof and legally permitted to further disclose the information or (e) which such part is required to disclose by law.

1.22 BIDDER RESPONSIBILITIES

The apparent winning Bidder shall be responsible for all equipment and services as required by this IFB. Subcontractors, if any, **MUST** be identified and a complete description of their role relative to the Bidder's submission **MUST** be included in the Bid Documentation.

1.23 BID AFFIDAVIT AND CONTRACT AFFIDAVIT

All bids must be accompanied by a completed Bid Affidavit (Appendix B). The Bidder also agrees that the Contract Affidavit (Appendix C) will be completed if selected for a contract award. The Contract Affidavit must be provided within five (5) business days after notification of proposed contract award. Copies of both affidavits are included in the appendices to this solicitation.

1.24 CONTRACT AGREEMENT

Appendix E includes a sample contract agreement that the apparent winning Bidder will be required to complete after contract award. The agreement will incorporate the following documents:

- Mandatory Contract Provisions (Appendix A)
- Bid Affidavit (Appendix B)
- Contract Affidavit (Appendix C)
- IFB0802, Section Three, Statement of Work
- Contractor's Bid Documentation
- Contractor's Bid Price Form (Appendix D)
- MBE Utilization Forms (Appendix F)
- Contractor's Service Agreement

By submitting a bid in response to this solicitation, a Bidder shall be deemed to have accepted the requirements of this IFB and the terms of the contract (Appendix E). Any exceptions to the requirements of the IFB or to the non-negotiable contract provisions will cause the bid to be rejected.

The State of Maryland's Mandatory Contract Provisions are included in Appendix A of this solicitation.

THE MANDATORY CONTRACT PROVISIONS ARE WRITTEN TO MEET THE PROCUREMENT LAWS AND REGULATIONS OF THE STATE OF MARYLAND. ALL BIDS THAT TAKE EXCEPTION TO THE NON-NEGOTIABLE PROVISIONS SHALL BE REJECTED AS NOT RESPONSIVE TO THE IFB.

THE PROCUREMENT LAW REFERENCED IS THE ANNOTATED CODE OF MARYLAND, STATE FINANCE AND PROCUREMENT ARTICLE AND THE REGULATIONS ARE STATE PROCUREMENT REGULATIONS, COMAR TITLE 21. VENDORS ARE ENCOURAGED TO FAMILIARIZE THEMSELVES WITH THE LAW AND REGULATIONS.

1.25 ORDER OF PRECEDENCE

In the event of any disputes or conflicts regarding the solicitation, the order of precedence shall be the Contract, the Invitation for Bids, and the Contractor's Bid Documentation and Bid Price Form.

1.26 ARREARAGES

By submitting a response to this solicitation, a Bidder shall be deemed to represent that it is not in arrears in the payment of any obligation due and owing the State of Maryland, including the payment of taxes and employee benefits, and that it shall not become so in arrears during the term of the contract if selected for contract award.

1.27 NON-VISUAL ACCESS

A Bidder must warrant that the information technology equipment to be provided as a result of its proposal (1) provides equivalent access for effective use by both visual and non-visual means; (2) will present information, including prompts used for interactive communications, in formats intended for both visual and non-visual use; (3) if intended for use in a network, can be integrated into networks for obtaining, retrieving, and disseminating information used by individuals who are not blind or visually impaired; and (4) is available, whenever possible, without modification for compatibility with software and hardware for non-visual access. The Bidder must further warrant that the cost, if any, of modifying the information technology for compatibility with software and hardware used for non-visual access will not increase the cost of the information technology by more than five percent. For purposes of this regulation, the phrase “equivalent access” means the ability to receive, use and manipulate information and operate controls necessary to access and use information technology by non-visual means. Examples of equivalent access include keyboard controls used for input and synthesized speech, Braille, or other audible or tactile means used for output.

1.28 BASIS FOR THE AWARD OF A CONTRACT

The contract award resulting from this solicitation will be made to the lowest responsive and responsible Bidder. Contract awards, if any, are subject to appropriate State approvals.

1.29 VERIFICATION OF REGISTRATION AND TAX PAYMENT

Before a corporation can do business in the State of Maryland it must be registered with the Department of Assessments and Taxation, State Office Building, Room 803, 301 West Preston Street, Baltimore, Maryland 21201. It is strongly recommended that any potential Bidder complete registration prior to the due date for receipt of proposals. A Bidder’s failure to complete registration with the Department of Assessments and Taxation may disqualify an otherwise successful Bidder from contract award.

1.30 FALSE STATEMENTS

Bidders are advised that Section 11-205.1 of the State Finance and Procurement Article of the Annotated Code of Maryland provides as follows:

In connection with a procurement contract a person may not willfully:

- Falsify, conceal, or suppress a material fact by any scheme or device;
- Make a false or fraudulent statement or representation of a material fact; or
- Use a false writing or document that contains a false or fraudulent statement or entry of a material fact.

A person may not aid or conspire with another person to commit an act under subsection (a) of Section 11-205.1.

A person who violates any provision of this section is guilty of a felony and on conviction is subject to a fine not exceeding \$20,000 or imprisonment not exceeding 5 years or both.

1.31 MINORITY BUSINESS ENTERPRISE (MBE) GOAL

A minority business enterprise subcontractor participation goal of **five (5%)** percent has been established for this solicitation. The contractor shall structure its awards of subcontracts under the contract in a good faith effort to achieve the goal in such subcontract awards by businesses certified by the State of Maryland as minority owned and controlled. MBE requirements are specified in Appendix F of this IFB.

A current directory of MBEs is available on the Maryland Department of Transportation website, http://www.mdot.state.md.us/MBE_Program/index.html.

If the Bidder has not proposed minority vendor participation of **five percent (5%)** or more, the Bidder **MUST** submit a statement so explaining. The State reserves the right to require the Bidder to make such additional efforts to secure MBE subcontractor participation as to assure the Bidder's good faith in attempting to meet this goal. **Completed and signed MBE Participation Forms (Appendix F, Attachments A and B) MUST be submitted with the Bid Documentation.**

1.32 LIVING WAGE REQUIREMENT

A solicitation for services under a State contract valued at \$100,000 or more may be subject to Title 18, State Finance and Procurement (SFP) Article, Annotated Code of Maryland. Additional information regarding the State's wage requirement is contained in this solicitation (see Appendix I entitled Living Wage Requirements for Service Contracts). If the Bidder fails to submit and complete the required documentation under State law, the State may determine a Bidder to be not responsible.

Contractors and Subcontractors subject to the Living Wage Law shall pay each covered employee at least \$11.30 per hour, if State contract services valued at 50% or more of the total value of the contract are performed in the Tier 1 Area. If State contract services valued at 50% or more of the total value are performed in the Tier 2 Area, a Bidder shall pay each covered employee at least \$8.50 per hour. The specific Living Wage rate is determined by whether a majority of services take place in a Tier 1 Area or Tier 2 Area of the State. The Tier 1 Area includes Montgomery, Prince George's, Howard, Anne Arundel, and Baltimore Counties, and Baltimore City. The Tier 2 Area includes any county in the State not included in the Tier 1 Area. In the event that the employees who perform the services are not located in the State, the head of the unit responsible for a State contract pursuant to §18-102 (d) shall assign the tier based upon where the recipients of the services are located.

The contract resulting from this solicitation has been deemed to be a Tier 1 contract.

**THE STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802**

**ACQUISITION OF
IBM TS3500 TAPE LIBRARIES AND
TS7740 VIRTUAL TAPE SYSTEM
FOR
THE ANNAPOLIS DATA CENTER**

SECTION TWO – BIDDER’S QUALIFICATIONS

2.0 LINE OF BUSINESS AND EXPERIENCE

- The Bidder must be an OEM certified business partner or the OEM.
- The Bidder or subcontractor must have 5 years experience installing and configuring the equipment bid or similar mainframe IBM tape system equipment.
- The Bidder or subcontractor must have 5 years experience providing maintenance and support 24 hours per day/7days per week for the equipment bid or similar mainframe IBM tape system equipment.
- The Bidder or subcontractor must have 2 years experience providing training for operators and technical support staff on the equipment bid or similar mainframe IBM tape system equipment.

**THE STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802**

**ACQUISITION OF
IBM TS3500 TAPE LIBRARIES AND
TS7740 VIRTUAL TAPE SYSTEM
FOR
THE ANNAPOLIS DATA CENTER**

SECTION THREE – STATEMENT OF WORK

This section is the Statement of Work for the contract resulting from this solicitation and details the mandatory hardware and support services that the Contractor shall be required to provide in its execution.

3.0 HARDWARE REQUIREMENTS

The Contractor shall provide the hardware detailed on the following list. All hardware shall be newly manufactured. The hardware shall have all components required to implement a Total Storage TS3500 Tape Library (4 frames) with High Availability dual accessors and a capacity of 597 cartridges for native zSeries and open systems for the Annapolis Data Center.

The hardware shall also include all components required to implement a Total Storage TS7740 Virtual Tape System for native zSeries tapes with 2TB cache.

The Contractor shall also provide an additional TS3500 Tape library with a capacity of at least 58 cartridges and two (2) TS1120 drives for the Baltimore office location.

QTY	DESCRIPTION
The following items are to be installed at the Annapolis Office Location (ADC)	
1	TS3500 Tape Library for Native zSeries tapes, 4 frames library that includes dual accessor service bays and high availability option (dual accessors)
10	IBM TS1120 tape drives for native (non-VTS) with encryption
4	IBM TS1120 tape drives for VTS zSeries with encryption
10	IBM TS1120 tape drives for open systems with encryption
1	3592-C06 controller with 2 FICON adapters
1	TS7740 (VTS) with 2 FICON adapter, 2 TB cache, 100MB/sec enabled
2	3593-L05 Library Managers
1	3953-F05 frame for controller and switches
2	2005-B32 IBM TotalStorage SAN32B-2 24 ports active, for open systems
12	2414 4 Gbps SW SFP Transceivers – 4, for open systems
48	5605 Fibre Cable LC/LC multimode (35m), for open systems
4	5605 Fibre Cable LC/LC multimode (5m), for open systems
60	3592 cleaning cartridges labeled
200	3592 300Gb tape cartridges initialized and labeled (600000-600199)
100	3592 300Gb tape cartridges initialized and labeled (T00000-T00999)
300	3592 300GB tape cartridges initialized and labeled (DS0000-DS0299) for open systems
The following items are to be installed at the Baltimore Office Location	
1	TS3500 Entry Level Capacity (58 slots active)
2	TS1120 Tape Drives
8	5605 Fibre Cable LC/LC multimode (2m) for open systems
1	3593-L05 Library Manager

3.1 DELIVERY REQUIREMENTS

The Contractor shall provide inside/in place delivery to the Annapolis Data Center, 108 Carroll Street, Annapolis, Maryland 21401, of all hardware within thirty (30) calendar days of contract execution. The delivery of all hardware shall be during the normal workweek (Monday through Friday) and normal work hours (8:00 a.m. to 4:00 p.m.). The Contractor shall coordinate and schedule the hardware delivery with the ADC Director of Operations Services. ADC has a loading lock limitation; the delivery trailer must not be longer than **forty-five (45)** feet.

The Contractor shall provide inside/in place delivery to the Comptroller's Baltimore office, 301 W. Preston Street, Baltimore, Maryland 21201, of all hardware within thirty (30) calendar days of contract execution. The delivery of all hardware shall be during the normal workweek (Monday through Friday) and normal work hours (8:00 a.m. to 4:00 p.m.). The Contractor shall coordinate and schedule the hardware delivery with the ADC Director of Operations Services.

3.2 CABLING REQUIREMENTS

As part of the systems assurance planning for installation of the new hardware (Section 3.4), the Contractor shall plan for the cable installations for both the Annapolis office and the Baltimore office with the ADC Director of Operation Services.

The Contractor shall execute the plan by furnishing, delivering and installing all FICON and Fibre Channel cables at either the Annapolis office and/or the Baltimore office.

3.3 INSTALLATION AND CONFIGURATION REQUIREMENTS

The Contractor shall assist with the installation and configuration of the hardware as well as customization of the z/OS operating system (currently v1.7) to support the TS3500 and TS7740.

The Contractor shall assist with the installation and configuration of the hardware as well as customization of the open systems equipment. This shall include configuration of the Windows Operating System and fibre connections between the TS1120 tape drives, fibre switches, and open systems backup servers.

The Contractor shall install all of the hardware within thirty (30) days of delivery.

3.3.1 HARDWARE

All hardware shall be installed by the Contractor at the Annapolis Data Center and Baltimore locations. The Contractor shall be responsible for relocating/moving all existing cables.

3.3.2 CUSTOMIZATION OF SOFTWARE AND MIGRATION SERVICES

The Contractor shall assist with the customization of the z/OS operating system (currently v1.7) and the Windows 2003 operating system required to support the TS3500s and the TS7740. The Contractor will assist in the migration from the ADC's current B18 VTS and ATL 3494. The Contractor shall perform the following tasks:

- Review and Recommend Service to be Applied
- Assist with the Application of Maintenance
- HCD/IOCP Generation
- IOCDS Coding
- LPAR Customization
- OAM
- ACS (SMS)
- Migration Planning
- Encryption
- Design a strategy for the Open Systems backups
- Fibre Switch Configuration

3.4 SYSTEM ASSURANCE AND IMPLEMENTATION PLANNING

The Contractor shall be responsible for providing systems assurance and implementation planning assistance that shall include review of power and HVAC requirements as well as maintenance, shipping clearances and floor loading for both the Annapolis and Baltimore locations. The ADC Director of Operation Services will assist with the systems assurance plan.

3.5 PERFORMANCE PERIOD OF ACCEPTANCE

After installation, configuration, and prior to acceptance by the State, both TS3500s and the TS7740 shall be subject to a period of performance not to exceed thirty (30) consecutive calendar days. The period will begin on the first full 24-hour day that occurs after ADC Management declares the installation and customization to be complete and the equipment to be online and operational.

During the thirty (30) day period, the hardware shall perform at a rate consistent with the performance specifications contained in the manufacturer's technical specifications. The equipment shall be online and operational 100 per cent of the time for thirty (30) consecutive calendar days, excluding normally scheduled preventive maintenance. The Contractor agrees and acknowledges that failure to satisfactorily complete the 30-day performance period of acceptance could result in termination of the contract requiring the Contractor to remove the equipment and, de-install any software components at no cost to the State.

Upon successful completion of the performance period of acceptance, the State shall deem the hardware fully installed and indicate its acceptance in a State's Letter of Acceptance to the Contractor. Upon receipt of said acceptance letter, the Contractor shall invoice the State for the installed hardware and all services rendered to date.

3.6 DE-INSTALLATION AND REMOVAL OF REPLACED HARDWARE

Upon successful completion of migration from the ATL 3494 and B18 VTS (which the State estimates could take up to one year) and the receipt of the State's Letter of Acceptance regarding the operation, performance and successful migration to the TS3500 and the TS7740 in a production environment, the Contractor shall cleanse the VTS cache of all its data, in accordance with the Maryland State IT Security Policy and Standards (See Appendix G).

After the cleansing process is complete, the vendor must de-install, pack, and take possession of the existing IBM ATL 3494 and IBM B18 VTS and, if deemed necessary by the State, relocate the TS3500 and the TS7740 within the ADC.

3.7 TRAINING REQUIREMENTS

Contractor shall provide for **160** instructor hours in 40 hour blocks (half in the first year and half over the life of the contract) of training for the TS3500 Tape Libraries and TS7740 including:

- operator interfaces
- operational modes and states
- displaying component status
- inserting tape cartridges
- manual mode of operation
- monitoring and reporting
- usage of encryption
- server backups
- fibre switch configuration.

Training will be at the ADC in Annapolis, Maryland. The allocation of training hours shall be at the discretion of the State. The State shall pay only for the training used at the Contractor's rates set out in the Bid Price Form.

3.8 DOCUMENTATION

The Contractor shall provide, upon delivery of the equipment, one (1) hardcopy and two (2) electronic or softcopy copies of all relevant IBM documentation to be supplied such as: Operator manuals, user manuals, and any other reference manuals.

3.9 WARRANTY AND MAINTENANCE

The Contractor shall provide warranty and maintenance (parts and labor) on all equipment for a period of five (5) years from the date of installation, which shall be defined as the day ADC management declares the installation to be complete, see section 3.5. The Contractor shall provide field service contract coverage twenty-four (24) hours a day, seven (7) days a week, including holidays. The Contractor shall have a service representative on site within two (2) hours of receiving a request for service from the ADC staff.

The new equipment shall have an automated feature that will monitor, detect and report (“call home”) any problems to its warranty/maintenance provider.

3.10 SECURITY REQUIREMENTS

A. The Contractor shall comply with and adhere to the Maryland State IT Security Policy and Standards (See Appendix G) as applicable to any Contractor’s activities and/or support. These policies may be revised from time to time and the Contractor shall comply with all such revisions.

B. Security Regarding Contractor-Owned Computer Equipment: The Contractor shall not connect their own equipment to the State's LAN/WAN without prior written approval by the State.

C. On-Site Security: Upon arrival on-site, all employees and/or agents of the Contractor shall register at the appropriate guard desk or with the appropriate State representative. When on-site, all employees and/or agents of the Contractor shall comply with all respective building and physical security rules for that particular location.

**THE STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802**

**ACQUISITION OF
IBM TS3500 TAPE LIBRARIES AND
TS7740 VIRTUAL TAPE SYSTEM
FOR
THE ANNAPOLIS DATA CENTER**

SECTION FOUR – BID FORMAT

The bid submission must include the following both in content and format.

4.0 BID FORMAT

Bidders must submit their bid package electronically as two separate files (may be zipped or unzipped) labeled in such a way as to identify which contains the Bid Documentation (example: BIDDERNAMEifb0802biddoc.xxx) and which contains the Bid Price Form (example: BIDDERNAMEifb0802bidform.xxx).

4.1.0 BID DOCUMENTATION

The file containing ‘Bid Documentation’ MUST incorporate the following:

- A. Transmittal Letter
- B. Confidential Declarations (see Sect. 1.21)
- C. Management Summary
- D. Bidder’s affirmation regarding its understanding of all requirements detailed in Sections Two and Three
- E. Completed MBE Utilization Forms (Appendix F, Attachments A and B)
- F. Completed Bid Affidavit (Appendix B)
- G. Completed Affidavit of Agreement regarding Maryland Living Wage Requirements (Appendix I).

4.1.1 TRANSMITTAL LETTER

A transmittal letter on the Bidder’s letterhead must accompany the file containing the ‘Bid Documentation.’ The sole purpose of this letter is to transmit the bid package and should contain original (scanned) signatures. The letter should be brief and should be signed by an individual who is authorized to bind the Bidder to all statements and requirements.

4.1.2 CONFIDENTIAL DECLARATIONS

As discussed in Section 1.21, a Bidder should give specific attention to the clear identification of those portions of its bid package that it considers confidential, proprietary commercial

information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Access to Public Records Act, Title 10, Subtitle 6, of the State Government Article of the Annotated Code of Maryland.

4.1.3 MANAGEMENT SUMMARY

The Bidder shall prepare and submit a “Management Summary” with its bid documentation. The summary shall provide a broad overview of the contents of the entire bid package. The Bidder should also include documentation of its status as a certified IBM Business Partner with the Management Summary and provide identification of all subcontractors and the work they will perform in the execution of any portion of the Statement of Work.

4.1.4 BIDDER’S AFFIRMATION OF ALL REQUIREMENTS DETAILED IN SECTION TWO AND SECTION THREE

The Bidder shall address each item in Section 2 -- Bidder's Qualifications -- and Section Three -- Statement of Work -- by affirmatively indicating its understanding of and ability to successfully meet **each** requirement.

4.1.5 BID AFFIDAVIT

The Bidder shall submit (scanned and in pdf/img format) a completed Bid Affidavit (Appendix B) that is signed and dated by an individual within its organization authorized to certify the statements contained therein.

4.1.6 MBE UTILIZATION / PARTICIPATION FORMS

The Bidder shall submit completed and signed MBE Participation Forms (Appendix F, Attachments A and B) with the file containing its Bid Documentation.

4.2.0 BID PRICE FORM

The Bid Price Form must include charges for the following (numbers in brackets represent corresponding paragraph in Section 3 of this IFB):

- Total Cost for all Hardware (Sect 3.0) and Cabling (Sect 3.2)
- Delivery of all Hardware and Cabling (3.1, 3.2)
- Planning & Installation of Hardware and Cabling, System Assurance (3.2, 3.3, 3.3.1, 3.4)
- Customization of Software and Migration Services (3.3.2)
- De-Installation, Packing & Disposal of Replaced Hardware (3.6)
- One Hundred Sixty (160) instructor hours of Training (3.7). Training must be priced in blocks of 40 instructor hours. The unit price for 40 hours must include any instructor-related expenses and be applicable to either on-site or off-site training. A total of Four (4) forty hour blocks must be bid.
- Documentation (3.8)

- Five Years On-Site Warranty & Maintenance (3.9). Payment schedule must be on an annual basis.

Less

- Trade-In Value of existing ATL serial numbers:

ATL HA1 frame	Serial Number	78-02106A
ATL L14 frame	Serial Number	78-16523
ATL D14 frame	Serial Number	78-34419
ATL D14 frame	Serial Number	78-34416
ATL D14 frame	Serial Number	78-34418
ATL D14 frame	Serial Number	78-34412
ATL S10 frame	Serial Number	78-47321
ATL S10 frame	Serial Number	78-47322
ATL HA1 frame	Serial Number	78-02106B
ATL D14 frame with drives	Serial Number	78-34431
3590 drive	Serial Number	B5304
3590 drive	Serial Number	B5270
3590 drive	Serial Number	B5189
3590 drive	Serial Number	B5217
3590 drive	Serial Number	B8557
3590 drive	Serial Number	B7881
ATL D14 frame with drives	Serial Number	78-34275
3590 drive	Serial Number	B5112
3590 drive	Serial Number	B5133
3590 drive	Serial Number	B4989
3590 drive	Serial Number	B5072
ATL D14 frame with drives	Serial Number	78-33862
3590 drive	Serial Number	B5186
3590 drive	Serial Number	B5319
3590 drive	Serial Number	B5341
3590 drive	Serial Number	B5292
3590 drive	Serial Number	DB851
3590 drive	Serial Number	DB804

- Trade-In Value of existing VTS serial numbers:

B18 VTS	Serial Number	78-71431
---------	---------------	----------

MANDATORY CONTRACT PROVISIONS

NON-HIRING OF EMPLOYEES: No employee of the State of Maryland whose duties as such employee include matters relating to or affecting the subject matter of this contract, shall, during the pendency and term of this contract and while so employed, become or be an employee of the contractor or any entity that is a subcontractor on this contract.

DISPUTES: This contract is subject to the provisions of State Finance and Procurement Article, Title 15, Subtitle 2, Annotated Code of Maryland and COMAR 21.10 (Administrative and Civil Remedies). Except as otherwise may be provided by law, all disputes arising under or as a result of a breach of this contract that are not disposed of by mutual agreement shall be resolved in accordance COMAR 21.07.01.06B. As used herein, "claim" means a written demand or assertion by one of the parties seeking, as a legal right, the payment of money, adjustment or interpretation of contract terms, or other relief, arising under or relating to this contract. A voucher, invoice, or request for payment that is not in dispute when submitted is not a claim under COMAR 21.07.01.06B. However, if the submission subsequently is not acted upon in a reasonable time or is disputed as to liability or amount, it may be converted to a claim for the purpose of COMAR 21.07.01.06B. A claim shall be made in writing and submitted to the procurement officer for decision in consultation with the Office of the Attorney General. When a claim cannot be resolved by mutual agreement, the contractor shall submit a written request for final decision to the procurement officer. The written request shall set forth all the facts surrounding the controversy. The contractor, at the discretion of the procurement officer, may be afforded an opportunity to be heard and to offer evidence in support of his claim. The procurement officer shall render a written decision on all claims within 180 days of receipt of the contractor's written claim, unless the procurement officer determines that a longer period is necessary to resolve the claim. If a decision is not issued within 180 days, the procurement officer shall notify the contractor of the time within which a decision shall be rendered and the reasons for such time extension. The decision shall be furnished to the contractor, by certified mail, return receipt requested, or by any other method that provides evidence of receipt. The procurement officer's decision shall be deemed the final action of the State. The procurement officer's decision shall be final and conclusive unless the contractor mails or otherwise files a written appeal with the Maryland State Board of Contract Appeals within 30 days of receipt of the decision. Pending resolution of the claim, the contractor shall proceed diligently with the performance of the contract in accordance with the procurement officer's decision.

MARYLAND LAW PREVAILS: This Contract shall be construed, interpreted, and enforced according to the laws of the State of Maryland.

AMENDMENT: This Contract constitutes the entire agreement between the parties and all other communications prior to its execution, whether written or oral, with reference to the subject matter of the Contract are superseded by this agreement. Any amendment to the Contract must first be approved in writing by the procurement officer, subject to any additional approvals required by Maryland law. No amendment to the Contract shall be binding unless so approved and unless it is in writing and signed by the party to be charged.

NONDISCRIMINATION IN EMPLOYMENT: The Contractor agrees: (a) not to discriminate in any manner against an employee or applicant for employment because of race, color, religion, creed, age, sex, marital status, national origin, ancestry, or physical or mental handicap unrelated in nature and extent so as reasonably to preclude the performance of such employment; (b) to include a provision similar to that contained in subsection (a), above, in any subcontract except a subcontract for standard commercial supplies or raw materials; and (c) to post and to cause subcontractors to post in conspicuous places available to employees and applicants for employment, notices setting forth the substance of this clause.

CONTINGENT FEE PROHIBITION: The contractor, architect, or engineer (as applicable) warrants that it has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee or agent working for the contractor, architect, or engineer, to solicit or secure this agreement, and that it has not paid or agreed to pay any person, partnership, corporation, or other entity, other than a bona fide employee or agent, any fee or any other consideration contingent on the making of this agreement.

MULTI-YEAR CONTRACTS CONTINGENT UPON APPROPRIATIONS: If the General Assembly fails to appropriate funds or if funds are not otherwise made available for continued performance for any fiscal period of this Contract succeeding the first fiscal period, this Contract shall be cancelled automatically as of the beginning of the fiscal year for which funds were not appropriated or otherwise made available; provided, however, that this will not affect either the State's rights or the Contractor's rights under any termination clause in this Contract. The effect of termination of the Contract hereunder will be to discharge both the Contractor and the State from future performance of the Contract, but not from their rights and obligations existing at the time of termination. The Contractor shall be reimbursed for the reasonable value of any non-recurring costs incurred but not amortized in the price of the Contract. The State shall notify the Contractor as soon as it has knowledge that funds may not be available for the continuation of this Contract for each succeeding fiscal period beyond the first.

TERMINATION FOR DEFAULT: If the Contractor fails to fulfill its obligations under this Contract properly and on time, or otherwise violates any provision of the Contract, the State may terminate the contract by written notice to the Contractor. The notice shall specify the acts or omissions relied upon as cause for termination. All finished or unfinished work provided by the Contractor shall, at the State's option, become the State's property. The State shall pay the Contractor fair and equitable compensation for satisfactory performance prior to receipt of notice of termination, less the amount of damages caused by the Contractor's breach. If the damages are more than the compensation payable to the Contractor, the Contractor will remain liable after termination and the State can affirmatively collect damages. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.11B.

TERMINATION FOR CONVENIENCE: The performance of work under this Contract may be terminated by the State, in accordance with this clause in whole, or from time to time in part, whenever the State shall determine that such termination is in the best interest of the State. The State will pay all reasonable costs associated with the contract that the Contractor has incurred up to the date of termination and all reasonable costs associated with termination of the Contract. However, the Contractor shall not be reimbursed for any anticipatory profits that have not been earned up to the date of termination. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.12A(2).

DELAYS AND EXTENSIONS OF TIME: The Contractor agrees to prosecute the work continuously and diligently and no charges or claims for damages shall be made by it for any delays or hindrances from any cause whatsoever during the progress of any portion of the work specified in this Contract. Time extensions will be granted only for excusable delays that arise from unforeseeable causes beyond the control and without the fault or negligence of the Contractor, including but not restricted to, acts of God, acts of the public enemy, acts of the State in either its sovereign or contractual capacity, acts of another Contractor in the performance of a contract with the State, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, or delays of subcontractors or suppliers arising from unforeseeable causes beyond the control and without the fault or negligence of either the Contractor or the subcontractors or suppliers.

VARIATIONS IN ESTIMATED QUANTITIES: No equitable adjustment shall be permitted in favor of either the State of Maryland or the Contractor in the event that the quantity of any pay item in this Contract is an estimated quantity and the actual quantity of such pay item varies from the estimated quantity stated in the Contract.

SUSPENSION OF WORK: The procurement officer unilaterally may order the Contractor in writing to suspend, delay, or interrupt all or any part of the work for such period of time as the procurement officer may determine to be appropriate for the convenience of the State.

PRE-EXISTING REGULATIONS: In accordance with the provisions of Section 11-206 of the State Finance and Procurement Article, Annotated Code of Maryland, the regulations set forth in Title 21 of the Code of Maryland Regulations (COMAR Title 21) in effect on the date of execution of this Contract are applicable to this Contract.

FINANCIAL DISCLOSURE: The Contractor shall comply with the provisions of Section 13-221 of the State Finance and Procurement Article of the Annotated Code of Maryland, which requires that every business that enters into contracts, leases, or other agreements with the State of Maryland or its agencies during a calendar year under which the business is to receive in the aggregate \$100,000 or more, shall, within 30 days of the time when the aggregate value of these contracts, leases or other agreements reaches \$100,000, file with the Secretary of State of Maryland certain specified information to include disclosure of beneficial ownership of the business.

POLITICAL CONTRIBUTION DISCLOSURE: The Contractor shall comply with Election Law Article, §§14-101 – 14-108, which requires that every person that enters into contracts, leases or other agreements with the State, a county, or an incorporated municipality, or their agencies, during a calendar year in which the person receives in the aggregate \$100,000 or more, shall file with the State Board of Elections a statement disclosing contributions in excess of \$500 made during the reporting period to a candidate for elective office in any primary or general election. The statement shall be filed with the State Board of Elections: (1) before a purchase or execution of a lease or contract by the State, a county, an incorporated municipality, or their agencies, and shall cover the preceding two calendar years; and (2) if the contribution is made after the execution of a lease or contract, then twice a year, throughout the contract term, on: (a) February 5, to cover the 6-month period ending January 31; and (b) August 5, to cover the 6-month period ending July 31.

RETENTION OF RECORDS: The Contractor shall retain and maintain all records and documents relating to this Contract for three years after final payment by the State hereunder or any applicable statute of limitations, whichever is longer, and shall make them available for inspection and audit by authorized representatives of the State, including the procurement officer or designee, at all reasonable times.

COMPLIANCE WITH LAWS: The Contractor hereby represents and warrants that:

- A. It is qualified to do business in the State of Maryland and that it will take such action as, from time to time hereafter, may be necessary to remain so qualified;
- B. It is not in arrears with respect to the payment of any monies due and owed to the State of Maryland, or any department or unit thereof, including but not limited to, the payment of taxes and employee benefits, and that it shall not become so in arrears during the term of this Contract;
- C. It shall comply with all federal, State and local laws, regulations, and ordinances, applicable to its activities and obligations under this Contract; and,
- D. It shall obtain, at its expense, all licenses, permits, insurance, and governmental approvals, if any, necessary to the performance of its obligations under this Contract.

COST AND PRICE CERTIFICATION: The Contractor by submitting cost or price information certifies that, to the best of its knowledge, the information submitted is accurate, complete, and current as of a mutually determined specified date prior to the conclusion of any price discussions or negotiations for: (1) A negotiated contract, if the total contract price is expected to exceed \$100,000, or a

smaller amount set by the procurement officer; or (2) A change order or contract modification, expected to exceed \$100,000, or a smaller amount set by the procurement officer. The price under this contract and any change order or modification hereunder, including profit or fee, shall be adjusted to exclude any significant price increases occurring because the Contractor furnished cost or price information which, as of the date agreed upon between the parties, was inaccurate, incomplete, or not current.

SUBCONTRACTING; ASSIGNMENT: The Contractor may not subcontract any portion of the services provided under this Contract without obtaining the prior written approval of the State of Maryland, nor may the Contractor assign this contract or any of its rights or obligations hereunder, without the prior written approval of the State. Any such subcontract or assignment shall be subject to any terms and conditions that the State deems necessary to protect its interests. The State shall not be responsible for the fulfillment of the Contractor's obligations to the subcontractors.

CHANGES IN SCOPE: The State shall retain the unilateral right to require changes in the scope of services provided under the Contract so long as such changes are within the general scope of work to be performed under the Contract.

PAYMENT OF STATE OBLIGATIONS: Payments to the Contractor pursuant to the Contract shall be made no later than 30 days after the State's receipt of a proper invoice from the Contractor. Each such invoice must reflect the Contractor's federal tax identification number. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1 of the State Finance and Procurement Article, Annotated Code of Maryland, or by the Public Service Commission of Maryland with respect to regulated public utilities, as applicable, are prohibited.

CONFLICTING TERMS: The Contractor understands and agrees that the terms and conditions of this Exhibit are mandatory under State law, may not be waived, and that they supersede any conflicting terms and conditions set forth in the Contract, which shall be deemed to be amended to incorporate therein the provisions set forth in this Exhibit.

CENTURY COMPLIANCE WARRANTY: Contractor warrants that the products provided or systems developed under this contract are century compliant. "Century compliant" means that the product: (1) is able to process date data accurately – including date data century recognition, calculations and accommodate same century and multi-century formulas and date values (including leap year factors), and date data interface values that reflect the century – when used either in a stand-alone configuration or in combination with other century compliant products used by the State; (2) will not abnormally terminate its function or provide or cause invalid or incorrect results due to incompatibility with the calendar year. In addition to any other warranties applicable to this contract or any remedies otherwise available to the State, Contractor agrees to repair or replace any product furnished under this Contract that is not century compliant, provided the State gives notice within a reasonable time following discovery of such failure.

NOVATION OR CHANGE OF NAME: This contract is not transferable or otherwise assignable without the written consent of the procurement officer, who, prior to granting consent, shall determine whether the proposed transfer or assignment is in the best interest of the State. If the procurement officer determines that the proposed transfer or assignment is in the best interest of the State, before the procurement officer consents to a transfer or assignment, the contractor (transferor) and the transferee shall enter into a novation agreement with the procurement officer in which the transferee agrees to complete the contract affidavit and assumes all of the transferor's obligations, and the transferor waives all rights under the contract as against the State. A contractor that intends to change its name shall notify the procurement officer and agree to enter into an agreement with the procurement officer that reflects the change of name and provides that no other terms of the contract are changed.

BID AFFIDAVIT

A. AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the (title) _____ and the duly authorized representative of (business) _____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

B. CERTIFICATION REGARDING COMMERCIAL
NONDISCRIMINATION

The undersigned bidder hereby certifies and agrees that the following information is correct: In preparing its bid on this project, the bidder has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not engaged in “discrimination” as defined in §19-103 of the State Finance and Procurement Article of the Annotated Code of Maryland. “Discrimination” means any disadvantage, difference, distinction, or preference in the solicitation, selection, hiring, or commercial treatment of a vendor, subcontractor, or commercial customer on the basis of race, color, religion, ancestry, or national origin, sex, age, marital status, sexual orientation, or on the basis of disability or any otherwise unlawful use of characteristics regarding the vendors, supplier’s or commercial customer’s employees or owners. “Discrimination” also includes retaliating against any person or other entity for reporting any incident of “discrimination”. Without limiting any other provision of the solicitation on this project, it is understood that, if the certification is false, such false certification constitutes grounds for the State to reject the bid submitted by the bidder on this project, and terminate any contract awarded based on the bid. As part of its bid or proposal, the bidder herewith submits a list of all instances within the past 4 years where there has been a final adjudicated determination in a legal or administrative proceeding in the state of Maryland that the bidder discriminated against subcontractors, vendors, suppliers, or commercial customers, and a description of the status or resolution of that determination, including any remedial action taken. Bidder agrees to comply in all respects with the State’s Commercial Nondiscrimination Policy as described under Title 19 of the State Finance and Procurement Article of the Annotated Code of Maryland.

C. AFFIRMATION REGARDING BRIBERY CONVICTIONS

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business (as is defined in §16-101(b) of the State Finance and Procurement Article of the Annotated Code of Maryland), or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities including obtaining or performing contracts with public bodies, has been convicted of, or has had probation before judgment imposed pursuant to Criminal Procedure Article, §6-220, Annotated Code of Maryland, or has pleaded nolo contendere to a charge of, bribery, attempted bribery, or conspiracy to bribe in violation of Maryland law, or of the law of any other state or federal law, except as follows (indicate the reasons why the affirmation cannot be given and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of person(s) involved, and their current positions and responsibilities with the business):

D. AFFIRMATION REGARDING OTHER CONVICTIONS

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities including obtaining or performing contracts with public bodies, has:

- (1) Been convicted under state or federal statute of:
 - (a) a criminal offense incident to obtaining, attempting to obtain, or performing a public or private contract; or
 - (b) fraud, embezzlement, theft, forgery, falsification or destruction of records, or receiving stolen property;
- (2) Been convicted of any criminal violation of a state or federal antitrust statute;

- (3) Been convicted under the provisions of Title 18 of the United States Code for violation of the Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. §1961, et seq., or the Mail Fraud Act, 18 U.S.C. §1341, et seq., for acts in connection with the submission of bids or proposals for a public or private contract;
- (4) Been convicted of a violation of the State Minority Business Enterprise Law, §14-308 of the State Finance and Procurement Article of the Annotated Code of Maryland;
- (5) Been convicted of a violation of the §11-205.1 of the State Finance and Procurement Article of the Annotated Code of Maryland;
- (6) Been convicted of conspiracy to commit any act or omission that would constitute grounds for conviction or liability under any law or statute described in subsection (1) through (5) above;
- (7) Been found civilly liable under a state or federal antitrust statute for acts or omissions in connection with the submission of bids or proposals for a public or private contract; or
- (8) Been found in a final adjudicated decision to have violated the Commercial Nondiscrimination Policy under Title 19 of the State Finance and Procurement Article of the Annotated Code of Maryland with regard to a public or private contract; or
- (9) Admitted in writing or under oath, during the course of an official investigation or other proceedings, acts or omissions that would constitute grounds for conviction or liability under any law or statute described in §§B — C and subsections (1) through (8) above, except as follows (indicate reasons why the affirmations cannot be given, and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of the person(s) involved and their current positions and responsibilities with the business, and the status of any debarment):

E. AFFIRMATION REGARDING DEBARMENT

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, controlling stockholders, or any of its employees directly involved in the business's contracting activities including obtaining or performing contracts with public bodies, has ever been suspended or debarred (including being issued a limited denial of participation) by any public entity, except as follows (list each debarment or suspension providing the dates of the suspension or debarment, the name of the public entity and the status of the proceedings, the name(s) of the person(s) involved and their current positions and responsibilities with the business, the grounds of the debarment or suspension, and the details of each person's involvement in any activity that formed the grounds of the debarment or suspension):

F. AFFIRMATION REGARDING DEBARMENT OF RELATED ENTITIES

I FURTHER AFFIRM THAT:

- (1) The business was not established and it does not operate in a manner designed to evade the application of or defeat the purpose of debarment pursuant to §16-101, et seq., of the State Finance and Procurement Article of the Annotated Code of Maryland; and
- (2) The business is not a successor, assignee, subsidiary, or affiliate of a suspended or debarred business, except as follows (you must indicate the reasons why the affirmations cannot be given without qualification):

G. SUB-CONTRACT AFFIRMATION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, has knowingly entered into a contract with a public body under which a person debarred or suspended under Title 16 of the State Finance and Procurement Article of the Annotated Code of Maryland will provide, directly or indirectly, supplies, services, architectural services, construction related services, leases of real property, or construction.

H. AFFIRMATION REGARDING COLLUSION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business has:

- (1) Agreed, conspired, connived, or colluded to produce a deceptive show of competition in the compilation of the accompanying bid or offer that is being submitted;
- (2) In any manner, directly or indirectly, entered into any agreement of any kind to fix the bid price or price proposal of the bidder or offeror or of any competitor, or otherwise taken any action in restraint of free competitive bidding in connection with the contract for which the accompanying bid or offer is submitted.

I. FINANCIAL DISCLOSURE AFFIRMATION

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, the provisions of §13-221 of the State Finance and Procurement Article of the Annotated Code of Maryland, which require that every business that enters into contracts, leases, or other agreements with the State of Maryland or its agencies during a calendar year under which the business is to receive in the aggregate \$100,000 or more shall, within 30 days of the time when the aggregate value of the contracts, leases, or other agreements reaches \$100,000, file with the Secretary of State of Maryland certain specified information to include disclosure of beneficial ownership of the business.

J. POLITICAL CONTRIBUTION DISCLOSURE AFFIRMATION

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, Election Law Article, §§14-101—14-108, Annotated Code of Maryland, which requires that every person that enters into contracts, leases, or other agreements with the State of Maryland, including its agencies or a political subdivision of the State, during a calendar year in which the person receives in the aggregate \$100,000 or more shall file with the State Board of Elections a statement disclosing contributions in excess of \$500 made during the reporting period to a candidate for elective office in any primary or general election.

K. DRUG AND ALCOHOL FREE WORKPLACE

(Applicable to all contracts unless the contract is for a law enforcement agency and the agency head or the agency head's designee has determined that application of COMAR 21.11.08 and this certification would be inappropriate in connection with the law enforcement agency's undercover operations.)

I CERTIFY THAT:

- (1) Terms defined in COMAR 21.11.08 shall have the same meanings when used in this certification.
- (2) By submission of its bid or offer, the business, if other than an individual, certifies and agrees that, with respect to its employees to be employed under a contract resulting from this solicitation, the business shall:
 - (a) Maintain a workplace free of drug and alcohol abuse during the term of the contract;
 - (b) Publish a statement notifying its employees that the unlawful manufacture, distribution, dispensing, possession, or use of drugs, and the abuse of drugs or alcohol is prohibited in the business' workplace and specifying the actions that will be taken against employees for violation of these prohibitions;
 - (c) Prohibit its employees from working under the influence of drugs or alcohol;

- (d) Not hire or assign to work on the contract anyone whom the business knows, or in the exercise of due diligence should know, currently abuses drugs or alcohol and is not actively engaged in a bona fide drug or alcohol abuse assistance or rehabilitation program;
- (e) Promptly inform the appropriate law enforcement agency of every drug-related crime that occurs in its workplace if the business has observed the violation or otherwise has reliable information that a violation has occurred;
- (f) Establish drug and alcohol abuse awareness programs to inform its employees about:
 - (i) The dangers of drug and alcohol abuse in the workplace;
 - (ii) The business' policy of maintaining a drug and alcohol free workplace;
 - (iii) Any available drug and alcohol counseling, rehabilitation, and employee assistance programs; and
 - (iv) The penalties that may be imposed upon employees who abuse drugs and alcohol in the workplace;
- (g) Provide all employees engaged in the performance of the contract with a copy of the statement required by §K(2)(b), above;
- (h) Notify its employees in the statement required by §K(2)(b), above, that as a condition of continued employment on the contract, the employee shall:
 - (i) Abide by the terms of the statement; and
 - (ii) Notify the employer of any criminal drug or alcohol abuse conviction for an offense occurring in the workplace not later than 5 days after a conviction;
- (i) Notify the procurement officer within 10 days after receiving notice under §K(2)(h)(ii), above, or otherwise receiving actual notice of a conviction;

- (j) Within 30 days after receiving notice under §K(2)(h)(ii), above, or otherwise receiving actual notice of a conviction, impose either of the following sanctions or remedial measures on any employee who is convicted of a drug or alcohol abuse offense occurring in the workplace:
 - (i) Take appropriate personnel action against an employee, up to and including termination; or
 - (ii) Require an employee to satisfactorily participate in a bona fide drug or alcohol abuse assistance or rehabilitation program; and
 - (k) Make a good faith effort to maintain a drug and alcohol free workplace through implementation of §K(2)(a)—(j), above.
- (3) If the business is an individual, the individual shall certify and agree as set forth in §K(4), below, that the individual shall not engage in the unlawful manufacture, distribution, dispensing, possession, or use of drugs or the abuse of drugs or alcohol in the performance of the contract.
- (4) I acknowledge and agree that:
- (a) The award of the contract is conditional upon compliance with COMAR 21.11.08 and this certification;
 - (b) The violation of the provisions of COMAR 21.11.08 or this certification shall be cause to suspend payments under, or terminate the contract for default under COMAR 21.07.01.11 or 21.07.03.15, as applicable; and
 - (c) The violation of the provisions of COMAR 21.11.08 or this certification in connection with the contract may, in the exercise of the discretion of the Board of Public Works, result in suspension and debarment of the business under COMAR 21.08.03.

L. CERTIFICATION OF CORPORATION REGISTRATION AND
TAX PAYMENT

I FURTHER AFFIRM THAT:

- (1) The business named above is a (domestic) (foreign) corporation registered in accordance with the Corporations and Associations Article, Annotated Code of Maryland, and that it is in good standing and has filed all of its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation, and that the name and address of its resident agent filed with the State Department of Assessments and Taxation is: Name:

Address: _____

(If not applicable, so state).

- (2) Except as validly contested, the business has paid, or has arranged for payment of, all taxes due the State of Maryland and has filed all required returns and reports with the Comptroller of the Treasury, the State Department of Assessments and Taxation, and the Department of Labor, Licensing, and Regulation, as applicable, and will have paid all withholding taxes due the State of Maryland prior to final settlement.

M. CONTINGENT FEES

I FURTHER AFFIRM THAT:

The business has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency working for the business, to solicit or secure the Contract, and that the business has not paid or agreed to pay any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency, any fee or any other consideration contingent on the making of the Contract.

N. Repealed.

O. ACKNOWLEDGEMENT

I ACKNOWLEDGE THAT this Affidavit is to be furnished to the Procurement Officer and may be distributed to units of: (1) the State of Maryland; (2) counties or other subdivisions of the State of Maryland; (3) other states; and (4) the federal government. I further acknowledge that this Affidavit is subject to applicable laws of the United States and the State of Maryland, both criminal and civil, and that nothing in this Affidavit or any contract resulting from the submission of this bid or proposal shall be construed to supersede, amend, modify or waive, on behalf of the State of Maryland, or any unit of the State of Maryland having jurisdiction, the exercise of any statutory right or remedy conferred by the Constitution and the laws of Maryland with respect to any misrepresentation made or any violation of the obligations, terms and covenants undertaken by the above business with respect to (1) this Affidavit, (2) the contract, and (3) other Affidavits comprising part of the contract.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By: _____

(Authorized Representative and Affiant)

CONTRACT AFFIDAVIT

A. AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the [title] _____ and the duly authorized representative of
[business] _____ and that I possess the legal authority to make this Affidavit on
behalf of myself and the business for which I am acting.

B. CERTIFICATION OF CORPORATION REGISTRATION AND TAX PAYMENT

I FURTHER AFFIRM THAT:

1. The business named above is a (domestic ____) (foreign ____) corporation registered in accordance with the Corporations and Associations Article, Annotated Code of Maryland, and that it is in good standing and has filed all of its annual reports together with filing fees, with the Maryland State Department of Assessments and Taxation, and that the name and address of its resident agent filed with the State Department of Assessments and Taxation is:

Name: _____

Address: _____.

2. Except as validly contested, the business has paid, or has arranged for payment of, all taxes due the State of Maryland and has filed all required returns and reports with the Comptroller of the Treasury, the State Department of Assessments and Taxation, and the Employment Security Administration, as applicable, and will have paid all withholding taxes due the State of Maryland prior to final settlement.

C. CERTAIN AFFIRMATIONS VALID

I FURTHER AFFIRM THAT:

To the best of my knowledge, information, and belief, each of the affirmations, certifications, or acknowledgments contained in that certain Bid/Proposal Affidavit dated _____, 20 __, and executed by me for the purpose of obtaining the contract to which this Exhibit is attached remains true and correct in all respects as if made as of the date of this Contract Affidavit and as if fully set forth herein.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By: _____
(Authorized Representative and Affiant)

**THE STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802**

BID PRICE FORM

DESCRIPTION	QTY	UNIT PRICE	EXT PRICE
TS3500 Automated Tape Library * (4 frames) with capacity for 597 tape cartridges in Annapolis * (1 frame) with capacity for 58 tape cartridges in Baltimore	2	\$	\$
IBM TS7740(VTS) with 2 FICON adapter, 2TB cache, 100MB/sec enabled	1	\$	\$
High Availability Option (dual accessors) for Annapolis	1	\$	\$
TS1120 tape drives * 10 non VTS in Annapolis * 4 VTS in Annapolis * 10 Open systems in Annapolis * 2 Open systems in Baltimore	26	\$	\$
3592-C06 controller with 2 FICON adapters for Annapolis	1	\$	\$
3593-L05 Library Managers * 2 in Annapolis * 1 in Baltimore	3	\$	\$
3593-F05 frame for controller and switches for Annapolis	1	\$	\$
2005-B52 IBM Total Storage SAN32B-2 24 ports active for open systems	2	\$	\$
2414 4 Gbps SW SFP Transceivers - 4 for open systems	12	\$	\$
3592 Cleaning cartridges labeled	60	\$	\$
3592-300 GB tape cartridges initialized and labeled * 200 (Labeled 600000-600199) * 100 (Labeled T00000-T00099) * 300 (Labeled DS0000-DS0299)	600	\$	\$

5605 Fibre Cable LC/LC multimode for open systems in Baltimore * 8 with a length of 2m for Baltimore * 4 with a length of 5m for Annapolis * 48 with a length of 35m for Annapolis * additional cables deemed necessary	60	\$	\$
(A) HARDWARE SUBTOTAL			\$
40-Hour Training Block (Instructor time)		4	\$
(B) TRAINING SUBTOTAL			\$
(C) DELIVERY CHARGES			\$
(D) PLANNING & INSTALLATION OF CABLING			\$
(E) INSTALLATION & CONFIGURATION OF HARDWARE AND SOFTWARE			\$
(F) CUSTOMIZATION OF z/OS HARDWARE AND SOFTWARE			\$
(G) MIGRATION SERVICES			\$
(H) DE-INSTALLATION & REMOVAL OF ATL and VTS			\$
(I) DOCUMENTATION			\$
Warranty / On-Site Maintenance Year 1		\$	
On-Site Maintenance Year 2		\$	
On-Site Maintenance Year 3		\$	
On-Site Maintenance Year 4		\$	
On-Site Maintenance Year 5		\$	
(J) 5 YRS WARRANTY & ON-SITE MAINTENANCE SUBTOTAL			\$
GRAND TOTAL (SUM OF A, B, C, D, E, F, G, H, I AND J)			\$
LESS TRADE IN CREDIT FOR ATL			\$
LESS TRADE IN CREDIT FOR VTS			\$
TOTAL AMOUNT OF BID			\$

Name of Bidder (Company):

Individual authorized to submit bid:

Signature:

Bidder Federal Tax ID No:

SAMPLE CONTRACT AGREEMENT

This agreement made the XX day of November, Two Thousand and Seven, by and between XXXX CORPORATION, STREET ADDRESS, CITY, STATE ZIP, Federal Employer Identification Number, xx-xxxxxx, (Contractor) and the STATE OF MARYLAND, acting by and through the Comptroller of Maryland (Customer),

Witnesseth, that for and in consideration of, the premises and the mutual promises herein contained, Contractor and Customer promise and agree as follows:

1. **Hardware, software and Support Services.** The Contractor shall furnish to Customer the hardware, software and support services described in the contract documents in accordance with, and subject to the terms and conditions of, the contract documents.
2. **Price and Payment.** Customer will pay for the hardware, software and support services to be provided in accordance with the terms and conditions of the contract documents and at the rates set forth in Exhibit D. Customer shall pay Contractor no later than thirty days after Customer receives a proper invoice from Contractor. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1, State Finance and Procurement Article, Maryland Code, are prohibited. Contractor's Federal Tax Identification Number (as noted in paragraph one of this Agreement) shall appear on all invoices submitted by the Contractor to the Customer for payment.
3. **Other Provisions.** Both parties are bound to and will abide by all terms and conditions of the contract documents.
4. **Mandatory Contract Provisions.** The Mandatory Contract Provisions attached hereto, as Appendix "A", are to be considered a part of this Agreement as though fully set forth herein. To the extent of any inconsistency or conflict between any provisions of this agreement and Appendix "A", the provisions Appendix "A" shall prevail.
5. **Contract Documents; Order of Precedence.** The contract ("Contract") between the parties is set forth in the contract documents, and supersedes all prior oral agreements and proposals. The contract documents consist of the documents set forth below; in the event of a conflict between the terms and conditions of any of the Contract Documents, the controlling terms shall be determined in the following order of priority:
 - Mandatory Contract Provisions - Exhibit A (IFB0802 Appendix "A")
 - This Agreement

Contract Agreement
Page Two

- Bid Affidavit - Exhibit B (IFB0802 Appendix “B”)
 - Contract Affidavit - Exhibit C (IFB0802 Appendix “C”)
 - Contractor’s Bid Package including Bid Price Form - Exhibit D (IFB0802 Appendix 'D')
 - IFB0802 - Exhibit E
 - Contractor Support Agreement - Exhibit F.
6. **Term of Contract.** This contract shall be effective upon approval by the Customer’s Board of Public Works and shall have a term of five years, beginning on XXXXX XX 2007 and terminating on XXX, 2012.
7. **Maryland Law Applies.** This contract shall be governed by and construed in accordance with the laws of the State of Maryland.

IN WITNESS WHEREOF, the parties have caused this agreement to be executed by their duly authorized officers, agents or officials.

XXXXX Corporation

COMPTROLLER OF MARYLAND

Signature

Signature

Printed Name

Printed Name

Title

Title

Date

Date

STATE OF MARYLAND
COMPTROLLER OF MARYLAND
INVITATION FOR BIDS NO. 0802

Minority Business Enterprise Participation

Purpose

Contractor shall structure its procedures for the performance of the work required in this contract to attempt to achieve the minority business enterprise (MBE) goal stated in Request for Bids No. 0802. MBE performance must be in accordance with this Exhibit, as authorized by Code of Maryland Regulations (COMAR) 21.11.03. Contractor agrees to exercise all good faith efforts to carry out the requirements set forth in this Exhibit.

MBE Goal

An MBE subcontract participation goal of 5 percent of the total contract dollar amount has been established for this procurement. By submitting a bid in response to this solicitation, the Bidder agrees that this dollar amount of the contract will be performed by certified minority enterprises.

Solicitation and Contract Formation

- A Bidder must include with its bid:
 1. A completed Certified MBE Utilization and Fair Solicitation Affidavit (Attachment A) whereby the Bidder acknowledges the certified MBE participation goal or requests a waiver, commits to make a good faith effort to achieve the goal, and affirms that MBE subcontractors were treated fairly in the solicitation process.
 2. A completed MBE Participation Schedule (Attachment B) whereby the Bidder responds to the expected degree of Minority Business Enterprise participation, as stated in the solicitation, by identifying the specific commitment of certified MBEs at the time of submission. The Bidder shall specify the percentage of contract value associated with each MBE subcontractor identified on the MBE Participation Schedule.

If a Bidder fails to submit, as required, Attachment A and Attachment B with its bid, the Procurement Officer shall deem the bid to be unresponsive.

- Within 10 working days from notification that it is the apparent winning bidder or from the date of the actual award, whichever is earlier, the apparent winning bidder must provide the following documentation to the Procurement Officer:
 1. Outreach Efforts Compliance Statement (Attachment C).
 2. Subcontractor Project Participation Statement (Attachment D).
 3. If the apparent winning bidder believes a waiver (in whole or in part) of the overall MBE goal is necessary, it must submit a fully documented waiver request that complies with COMAR 21.11.03.11.
 4. Any other documentation required by the Procurement Officer to ascertain the bidder's responsibility in connection with the certified MBE participation goal.

If the apparent winning bidder fails to return each completed document within the required time, the Procurement Officer may determine that the apparent winning bidder is

not responsible and therefore not eligible for contract award. If the contract has already been awarded, the award is voidable.

Contract Administration Requirements

Contractor shall:

1. Submit monthly to the Department a report listing any unpaid invoices, over 30 days old, received from any certified MBE subcontractor, the amount of each invoice and the reason payment has not been made.
2. Include in its agreements with its certified MBE subcontractors a requirement that those subcontractors submit monthly to the Department a report that identifies the prime contract and lists all payments received from Contractor in the preceding 30 days, as well as any outstanding invoices, and the amount of those invoices.
3. Maintain such records as are necessary to confirm compliance with its MBE participation obligations. These records must indicate the identity of certified minority and non-minority subcontractors employed on the contract, the type of work performed by each, and the actual dollar value of work performed. Subcontract agreements documenting the work performed by all MBE participants must be retained by the Contractor and furnished to the Procurement Officer on request.
4. Consent to provide such documentation as reasonably requested and to provide right-of-entry at reasonable times for purposes of the State's representatives verifying compliance with the MBE participation obligations. Contractor must retain all records concerning MBE participation and make them available for State inspection for a period of three years after final completion of the contract.
5. At the option of the procurement agency, upon completion of the contract and before final payment and/or release of retainage, submit a final report in affidavit form and under penalty of perjury, of all payments made to, or withheld from MBE subcontractors.

ATTACHMENTS

- A. Certified MBE Utilization and Fair Solicitation Affidavit (must be submitted with bid)
- B. MBE Participation Schedule (must be submitted with bid)
- C. Outreach Efforts Compliance Statement (must be submitted within 10 working days of notification of apparent winning bid or actual award, whichever is earlier)
- D. Subcontractor Project Participation Statement (must be submitted within 10 working days of notification of apparent winning bid or actual award, whichever is earlier).

CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION

AFFIDAVIT

(This document must be included with the offer. If the Bidder fails to submit this form with the bid as required, the Procurement Officer shall deem the Bidder as unresponsive)

In conjunction with the bid submitted in response to Invitation for Bids (IFB) No. 0802, I affirm the following:

1. I acknowledge the certified Minority Business Enterprise participation goal of 5 percent and commit to make a good faith effort to achieve this goal.

OR

After having made a good faith effort to achieve the MBE participation goal, I conclude I am unable to achieve it. Instead, I intend to achieve MBE participation of _____% and request a waiver of the remainder of the goal. Within 10 business days of receiving notice that our firm is the apparent winning bidder, I will submit a written waiver request that complies the COMAR 21.11.03.11. I acknowledge that the MBE subcontractors / suppliers listed in the MBE Participation Schedule will be used to accomplish the percentage of MBE participation that I intend to achieve.

2. I have identified the specific commitment of certified MBEs by completing and submitting an MBE Participation Schedule with the bid.
3. I understand that if I am notified that I am the apparent winning vendor, I must submit the following documentation with 10 working days of receiving notice of the potential award or from the date of actual award, whichever is earlier (COMAR 21.11.03.10).
 - (a) Outreach Efforts Compliance Statement (Attachment C).
 - (b) Subcontractor Project Participation Statement (Attachment D).
 - (c) MBE Waiver Request per COMAR 21.11.03.11 (if applicable).
 - (d) Any other documents required by the Procurement Officer to ascertain Bidder's responsibility in connection with the certified MBE participation goal.

I acknowledge that if I fail to return each completed document within the required time, the Procurement Officer may determine that I am not responsible and therefore not eligible for contract award. If the contract has already been awarded, the award is voidable.

4. In the solicitation of subcontract quotations or offers, MBE subcontractors were provided not less than the same information and amount of time to respond as were non-MBE subcontractors.

I solemnly affirm under the penalties of perjury that the contents of this paper are true to the best of my knowledge, information, and belief.

Offeror Name

Signature of Affiant

Address

Printed Name, Title

Date

SUBMIT THIS AFFIDAVIT WITH PROPOSAL

MBE PARTICIPATION SCHEDULE

(This document must be included with the offer. If the Bidder fails to submit this form with the proposal as required, the Procurement Officer shall deem the Bidder to be non-responsive)

Prime Contractor (Firm Name, Address, Phone)	Project Description
Project Number	
List Information For Each Certified MBE Subcontractor On This Project	
A. Minority Firm Name, Address, Phone	MBE Certification Number:
Work To Be Performed	
Percentage of Total Contract	
B. Minority Firm Name, Address, Phone	MBE Certification Number:
Work To Be Performed	
Percentage Of Total Contract	
C. Minority Firm Name, Address, Phone	MBE Certification Number:
Work To Be Performed	
Percentage Of Total Contract	

SUMMARY

TOTAL MBE PARTICIPATION: _____%

TOTAL AFRICAN-AMERICAN MBE PARTICIPATION: _____%

TOTAL WOMAN-OWNED MBE PARTICIPATION: _____%

Document Prepared by: (please print or type)

Name: _____ Title: _____

OUTREACH EFFORTS COMPLIANCE STATEMENT

In conjunction with the bid submitted in response to IFB0802, I state the following:

1. Bidder identified opportunities to subcontract in these specific work categories:

2. Attached to this form are copies of written solicitations (with bidding instructions) used to solicit certified MBEs for these subcontracting opportunities.

3. Bidder made the following attempts to personally contact the solicited MBEs:

4. ☐ Bidder assisted MBEs to fulfill or to seek waiver of bonding requirements.

IFB0802 - N/A

☐ This project does not involve bonding requirements.

5. ☐ Bidder did / did not attend pre-bid conference.

Bidder Name

By:

Address

Name, Title

Date

SUBCONTRACTOR PROJECT PARTICIPATION STATEMENT

SUBMIT ONE FORM FOR EACH CERTIFIED MBE LISTED IN THE MBE PARTICIPATION SCHEDULE

Provided that _____ is awarded the State contract in conjunction
Prime Contractor Name

with IFB0802, it and _____, MDOT Certification No. _____,
Subcontractor Name

intend to enter into a contract by which Subcontractor shall: (describe work)

- ☐ No bonds are required of Subcontractor
- ☐ The following amount and type of bonds are required of Subcontractor:

Prime Contractor Signature

By: _____
Name, Title

Date

Subcontractor Signature

By: _____
Name, Title

Date



**Department of Budget and Management
Office of Information Technology**

**Information Technology
Security Policy and Standards**

Version 1.5

January 2007

Table of Contents

INTRODUCTION	4
1 INFORMATION TECHNOLOGY SECURITY POLICY	5
1.1 SCOPE	5
1.2 OBJECTIVES	5
1.3 PREVIOUS POLICY SUPERSEDED	5
1.4 AUTHORITY	5
1.5 COMPLIANCE	6
1.6 SECURITY PROGRAM MAINTENANCE AND REVIEW	6
1.7 INFORMATION TECHNOLOGY SECURITY DEVIATION AND RISK ACCEPTANCE	6
2 KEY DEFINITIONS	7
3 RESPONSIBILITY STANDARD	9
3.1 STATE CHIEF OF INFORMATION TECHNOLOGY	9
3.2 DIVISIONS OF SECURITY AND ENTERPRISE ARCHITECTURE, DBM OIT	9
3.3 AGENCY RESPONSIBILITIES	10
3.4 EMPLOYEES AND CONTRACTORS	10
4 INFORMATION TECHNOLOGY SECURITY PROGRAM STANDARD	11
4.1 IT SECURITY POLICY	11
4.2 RISK MANAGEMENT	11
4.3 SYSTEMS DEVELOPMENT LIFE CYCLE METHODOLOGY	11
4.4 IT SECURITY CERTIFICATION & ACCREDITATION	11
4.5 IT DISASTER RECOVERY PLANNING	12
4.6 IT SECURITY AWARENESS, TRAINING, AND EDUCATION	12
4.7 IT INCIDENT RESPONSE PROCESS	12
4.8 EXTERNAL CONNECTIONS REVIEW	12
4.9 IT SECURITY PROGRAM REPORTING	12
5 NONPUBLIC INFORMATION STANDARD	13
5.1 SYSTEM SENSITIVITY DESIGNATION	13
6 ACCESS CONTROL STANDARD	14
6.1 AUTHENTICATION	14
6.2 PASSWORD CONSTRUCTION RULES AND CHANGE REQUIREMENTS	14
6.3 AUTHORIZATION	15
6.4 AUDIT TRAIL	15
6.5 VIOLATION LOG MANAGEMENT AND REVIEW	16
7 NETWORK SECURITY STANDARD	17
7.1 DIAL-IN ACCESS	17
7.2 BANNER TEXT	17
7.3 FIREWALLS & NETWORK DEVICES	18
7.4 INTRUSION DETECTION SYSTEMS	18
7.5 SERVICE INTERFACE AGREEMENT	18
7.6 TELEWORKING	19
7.7 MOBILE CODE	19
7.8 WIRELESS NETWORKS	19
7.9 PRIVATE BRANCH EXCHANGE (PBX)	20
7.10 FACSIMILE	20
8 PHYSICAL SECURITY STANDARD	21
8.1 SECURED IT AREAS	21
8.2 STORAGE MEDIA DISPOSAL	21
8.3 MEDIA REUSE	21
8.4 STORAGE AND MARKING	22
8.5 PERSONNEL	22
9 MICROCOMPUTER/PC/LAPTOP SECURITY STANDARD	23
9.1 GENERAL CONTROLS	23
9.2 SOFTWARE LICENSES AND USE	23
9.3 LAPTOP SECURITY AND MOBILE COMPUTING	23

9.4	PERSONALLY OWNED DATA PROCESSING EQUIPMENT	24
10	ENCRYPTION STANDARD	25
10.1	PUBLIC KEY TECHNOLOGY (ASYMMETRIC)	25
11	IT INFORMATION SECURITY DEVIATION/RISK ACCEPTANCE STANDARD	26
11.1	GENERAL REQUIREMENTS	26
12	USE OF ELECTRONIC COMMUNICATIONS STANDARD	27
12.1	INTERNET AND ELECTRONIC COMMUNICATIONS	27
12.2	COMPUTER SOFTWARE AND COPYRIGHT INFRINGEMENT	27
12.3	IT INCIDENT AND ADVISORIES	27
13	RECORD OF REVISIONS.....	28

Introduction

This document provides policy and supporting standards for information technology (IT) security. The policy applies to Executive agencies of the State of Maryland, and establishes general requirements and responsibilities for protecting technology systems, including the responsibility for each agency to have its own technology security plan. The standards establish minimum levels of compliance.

The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, and many other more specialized resources. The policy is necessitated by the State's use of IT to help carry out nearly all of its public services and internal operations. The State's delivery of critical public services depends on the availability, reliability and integrity of its IT systems. Therefore each agency must adopt appropriate methods to protect its technology systems. While some agencies will need to adopt stronger standards and methods, the statewide program based on this policy provides the minimum requirements and a consistent approach for security.

The common security approach also supports compatible security solutions shared among agencies, yielding a better return on technology investment. The security policy and standards will evolve and will require regular updates to remain current.

The Secretary of the Department of Budget and Management issues the policy and standards under authority granted by the Annotated Code of Maryland, Finance and Procurement Article § 3-401 through 3-413 and § 3-701 through 3-705. The Office of Information Technology within the Department of Budget and Management administers the policy.

Persons with questions or needing further information are encouraged to contact the Information Technology Security Officer in the Office of Information Technology (410 260-7778).

Section: 1	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

1 Information Technology Security Policy

Information and information technology systems are essential assets of the State of Maryland. They are vital to the citizens of the State. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as to local and federal government entities and to other State agencies. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Each agency of the Executive Branch of the State is responsible for compliance with this policy and these standards. The Office of Information Technology (OIT) of the Department of Budget and Management and agency IT components are to use this policy and these standards as a guide when procuring IT services, service providers, contractors, software, hardware and network components.

1.1 Scope

This policy covers all information that is electronically generated, received, stored, printed, filmed, and typed. In accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, the provisions of this policy apply to:

- All units of the Executive Branch of the State of Maryland for all of their IT systems regardless of who is operating them;
- All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights.

1.2 Objectives

This policy and these standards define the minimum requirements to which each State agency, including employees and contractors, must adhere. The primary objectives of the IT Security Policy are:

- To establish a secure environment for the processing of data;
- To reduce information security risk;
- To communicate the responsibilities for the protection of information.

1.3 Previous Policy Superseded

This policy and these standards supersede the policies and standards as previously stated in the “State Agency Data Systems Security Practices” as revised (1999).

1.4 Authority

The Office of Information Technology of the Department of Budget and Management has authority to set policy and provide guidance and oversight for security for all IT systems in accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705.

1.5 Compliance

The head of each agency is responsible for compliance with and enforcement of this policy. Agency Chiefs of Information Technology (CITs) shall develop and implement an Agency IT Security Program to implement this policy and these standards. Where the agency's IT Security Program is unable to comply with this policy, a timetable to resolve the discrepancies and controls for compliance shall be included. The controls shall include but are not limited to:

- Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services;
- Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed;
- Ensuring that risks to information security are identified and controls implemented to mitigate these risks;
- Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards;
- Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations;
- Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's IT assets.

1.6 Security Program Maintenance and Review

Each State agency will review and update its IT Security Program as needed to conform to changes within the agency or in the State IT Security Program. Refer to NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems for additional guidance: <http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>. The status of agency IT Security Programs Systems shall be reported according to Section 4.9.

1.7 Information Technology Security Deviation and Risk Acceptance

Compliance with this policy shall be planned and achieved as promptly as possible. When an agency determines, in the course of planning or carrying out its IT Security Program, that it is not feasible or practical to comply with a provision or provisions of this policy and attendant standards, or to do so promptly, it shall document the deviation from policy or standards. The documentation, with a timetable for compliance when practicable, shall be prepared as an IT Security Deviation Request.

IT Security Deviation Requests must be filed in accordance with the specifications detailed in the State IT Security Deviation/Risk Acceptance Standard (see Section 11, IT Security Deviation/Risk Acceptance Standard). Such deviations require the approval of the agency CIT, the agency head and the State CIT.

Section: 2	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

2 Key Definitions

Term / Acronym	Definition
Acceptable Risk	A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accountability	A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.
Accreditation	The authorization and approval granted to operate a system or network in order to process sensitive data in an operational environment.
Agency	All units of the Executive branch excluding the University System of Maryland.
Authentication	The testing or reconciliation of evidence of a user's identity.
Authorization	The rights and permissions granted to an individual (or process), which enables access to a computer resource.
Authorized Software	Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.
Availability	Ensures the reliable and timely access to data or computing resources by the appropriate personnel.
Certification	A technical review made as part of and in support of the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. A judgment and statement of opinion that the accrediting official can use to officially accredit the system is produced.
CIT	Chief of Information Technology.
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical systems.
Computer	An electronic, magnetic, optical, or other data processing device or system that performs logical, arithmetic, memory, or storage functions. It includes any data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.
Confidentiality	Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.
Data Remanence	Residual information left behind once media has been in some way erased.
Incident	Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.
Identification	Data uniquely labeling a user to a system.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Information	The business function owner responsible for the information assets for a particular IT

Term / Acronym	Definition
Custodian	System.
Integrity	Freedom from corruption or unauthorized modification; internal and external consistency.
IT Systems	Automated systems: communications systems including wireless systems, computer systems, hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.
ITEPP	Information Technology Emergency Preparedness Plan, including the business continuity plan, the recovery plan and the business resumption plan.
MCERT	Maryland's Computer Emergency Response Team. Team to be activated in the event of a major IT related disaster.
Mobile Code	Code that can be transmitted across the network and executed by a recipient.
Network	A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.
Untrusted Network	Any network not controlled by the State agency.
NIST	National Institute of Standards and Technology.
Nonpublic	Nonpublic is information that is not subject to inspection and copying under the Maryland Public Information Act or federal law.
Non-repudiation	Authentication with a high assurance to be genuine and that can not subsequently be refuted.
OIT	Office of Information Technology within the Department of Budget and Management.
Perimeter Access	Access to all entry and exit points of the network, controlled by firewalls and other filtering mechanisms.
Policy	For purposes of this document means both Policy and Standards
Privacy	Information that is free from unauthorized intrusion.
Public	Information that may be inspected and copied under the Maryland Public Information Act.
Residual Risk	The portion of risk that remains after security measures have been applied.
Risk	The probability that a particular threat will exploit a particular vulnerability of an IT System.
SDLC	Systems Development Life Cycle as defined in the State of Maryland SDLC Methodology (http://www.dbm.maryland.gov/ Keyword: SDLC).
SIA	Service Interface Agreement
Software	Computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.
VoIP	Voice over Internet Protocol, providing telephony services over IP networks.

Section: 3	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

3 Responsibility Standard

The following standard sets the minimum level of responsibility for the following individuals and/or groups:

- State CIT;
- Divisions of Security and Enterprise Architecture for OIT;
- Agency;
- Employees and Contractors.

3.1 State Chief of Information Technology

The duties of the State CIT are:

- Providing Statewide IT security policy, standards, guidelines, and procedures;
- Ensuring the State's IT Security Program is established and implemented in compliance with State laws and regulations and federal laws where applicable;
- Approving deviations to IT security requirements;
- Reporting to the Governor and the Legislature on the status of the State's IT Security Program;
- Enforcing State security policy, including establishing the appropriate measures and remedial actions for agencies for non-compliance.

3.2 Divisions of Security and Enterprise Architecture, DBM OIT

These divisions are responsible for:

- Developing and maintaining a Statewide Security Program that includes policy, standards, guidelines, procedures, best security practices, IT disaster recovery planning guidelines, IT Security Certification and Accreditation guidelines, security awareness training, and an incident response reporting capability;
- Identifying security vulnerabilities in State systems and recommending corrective action;
- Ensuring IT Disaster Recovery plans for critical IT Systems are maintained and that plans are exercised at least annually;
- Developing and maintaining a Statewide security architecture;
- Coordinating with State agency CIT's, federal and local government, and private industry to resolve security issues and improve security for State systems;
- Provide the appropriate guidance to assist agencies in establishing IT Security Programs and compliance with IT Security Policy;
- Working with other State agencies to establish a coordinated computer incident response effort.

3.3 Agency Responsibilities

Each agency is responsible for:

Ensuring the agency's IT security program is established and implemented in compliance with State security policies and standards, State and Federal laws and regulations as applicable:

- Implementing an IT Security Certification and Accreditation process for the life cycle of each agency critical IT System;
- Reporting to the OIT on the status of the agency's IT Security Program
- Enforcing the State IT Security Policy;
- Managing the program and initiating measures to assure and demonstrate compliance with security requirements;
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions;
- Assuming the lead role in resolving security and privacy incidents;
- Documenting and ensuring that a process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard;
- Specifying the level of security required to protect all information assets under their control to comply with this Policy;
- Generating any IT Information Security Deviation/Risk Acceptance request in accordance with Section 11;
- Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
- Ensuring a configuration/change management process is used to maintain the security of the IT system;
- Administering a virus prevention and incident reporting program that coordinates with Maryland's Computer Incident Response Team;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users.

3.4 Employees and Contractors

All employees and contract personnel are responsible for:

- Being aware of their responsibilities for protecting IT assets of their agency and the State;
- Exercising due diligence in carrying out the IT Security Policy;
- Being accountable for their actions relating to their use of all IT Systems;
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State.

Section: 4	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

4 Information Technology Security Program Standard

Each agency is responsible for developing an IT Security Program for securing the agency's communications systems, computer systems, networks, and data in accordance with the State IT Security Policy. The status of an agency IT Security Program will be reported to the State CIT on an annual basis. This standard specifies the major components that must be included in every IT Security Program. The following list is not exhaustive; it functions as the minimum set of requirements. At a minimum each program must contain the following elements:

- IT Security Policy;
- Risk Management;
- Systems Development Life Cycle Methodology;
- IT Security Certification and Accreditation;
- IT Disaster Recovery Planning;
- IT Security Awareness Training;
- IT Incident Response Process;
- External Connections Review;
- IT Security Program Reporting.

4.1 IT Security Policy

Each agency must have a written IT security policy, with standards, and procedures. The agency policy must meet the minimum requirements as set forth in this policy.

4.2 Risk Management

A risk management process must be implemented to assess the acceptable risk to agency IT systems as part of a risk-based approach used to determine adequate security for the system. Agencies shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Agencies will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system (see Section 5, Nonpublic Information Standard). Refer to NIST Special Publication 800-30, Risk Management Guide for Information Technology for guidance: <http://csrc.nist.gov/publications/nistpubs/>.

4.3 Systems Development Life Cycle Methodology

All State systems must include IT security as part of the system development life cycle management process. Refer to the requirements in the State of Maryland SDLC Methodology: <http://www.dbm.maryland.gov/>; Keyword: SDLC.

4.4 IT Security Certification & Accreditation

Agencies shall develop and implement an IT security certification and accreditation program as part of an overall IT risk management strategy. The program will maintain a catalog of all IT systems and sites (to include existing), ranked by sensitivity and criticality. The cataloged items should be certified and accredited, in order, according to State IT Security Certification and Accreditation (C&A) Guidelines. All new development shall be conducted using the IT Security C&A process integrated into the development process.

4.5 IT Disaster Recovery Planning

Agencies shall develop, implement, and test an IT Disaster Recovery plan for each critical IT system to ensure that a contingency system will be available in the event of a disaster to the primary production system. Reference State IT Disaster Recovery Guidelines.

4.6 IT Security Awareness, Training, and Education

Agencies shall develop and implement a security awareness, training, and education program for all agency employees and contractors to ensure that all employees and contractors adhere to the State IT Security Policy. Reference State IT Security Awareness Training and Education Training Guidelines.

4.7 IT Incident Response Process

Agencies shall be required to participate in the State Incident Response Process by detecting, tracking, logging, and reporting security incidents. Reference Maryland Computer Incident Response Capability Procedures and Standard Operation Procedures for Electronic Evidence Handling.

4.8 External Connections Review

External network connections, non-networked computers and dial-in connections shall be managed, reviewed annually, and documented as prescribed by the Agency IT Security Program. Results will be reported annually.

4.9 IT Security Program Reporting

Each agency is responsible for reporting on the status of the agency IT Security Program the DBM/OIT Security Division on an annual basis. A project plan detailing the projects, estimated costs, and estimated completion time required to bring the agency into compliance with the IT Security Policy must be included in the annual report.

Section: 5	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

5 Nonpublic Information Standard

Agencies shall establish and document a process that protects nonpublic information from disclosure to unauthorized individuals or entities, including other State or federal agencies. The process shall be compliant with the Maryland Public Information Act and any applicable federal laws.

5.1 System Sensitivity Designation

Each agency must specify corresponding classification and controls that must be in place for the data within that agency. When the IT System is shared between State units and/or between State, Federal, or local units the highest level of classification will determine the classification of the data or IT System. For example, one agency may categorize the data at a medium level while the second agency may classify the data at a basic level; therefore, the data at both agencies will be at a medium level. All parties sharing the IT System or data must agree to the initial classification and any change in the classification. An IT System shall clearly identify data that is considered non-public or public and any electronic exchange of data will clearly state that the information is non-public or public.

Section: 6	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

6 Access Control Standard

All Agencies must ensure that information is accessed by the appropriate persons for authorized use only. To help accomplish this each agency must establish at a minimum the following:

- An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system;
- An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of “least possible privileges” and “need-to-know”;
- An audit trail process to ensure accountability of system and security-related events;
- A process for ensuring that all systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, this capability must be enabled at all times;
- A review process of security audit logs, incident reports and on-line reports at least one (1) time per business day using automated tools to facilitate the review where possible;
- An investigation process for any unusual or suspicious items, which will incorporate reporting the results as specified in the State IT Incident Response Guideline;
- An internal assessment process for verifying their compliance to the State IT Security Policy;
- The processes to establish, manage, and document user id and password administration;
- A review of access privileges on an annual basis;
- A process for protecting nonpublic information;
- A process for explicitly authorizing access to nonpublic information;
- A process for documenting and escalating all instances of non-compliance with the State IT Security Policy;
- A segregation of the functions of system administration and security administration to provide separation of duties;
- Procedures prohibiting security personnel from initiating, programming, processing or authorizing business transactions;
- Independent audits of agency security administrators’ security transactions.

6.1 Authentication

All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as “Functional ids”. Functional ids are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., RACF id used to run production jobs). Passwords associated with functional ids are exempt from the password restriction on sharing and change requirements specified below.

6.2 Password Construction Rules and Change Requirements

Passwords must meet the following usage, construction and change requirements:

- The password must not be the same as the user id;
- Passwords must never be displayed on the screen;
- The user must select passwords unless randomly generated. Initial passwords and password sets distributed to the user must be issued “pre-expired” forcing the user to change them upon logon;
- Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic and

numeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters;

- Passwords must not contain leading or trailing blanks;
- Passwords must not contain more than two (2) consecutive identical characters;
- Password reuse must be prohibited by not allowing the last 10 passwords to be reused with a minimum password age of at least 2 days;
- Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
- Automated controls must ensure that passwords are changed at least as frequently as every ninety (90) days for regular users, forty-five (45) days for power users, such as network and database administrators;
- Passwords older than its expiration date must be changed before any other system activity is performed;
- User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts while allowing a minimum of a ten (10) minute automatic reset of the account;
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

6.3 Authorization

All Agencies must have the following authorization controls implemented:

- A documented process to ensure that access privileges are verified at least annually;
- An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity;
- A documented process to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hours of the change;
- A documented process to ensure that physical and logical access is immediately disabled upon a change in employment status where appropriate;
- An automated process to ensure that user ids are disabled after sixty (60) days of inactivity unless they are extended through the explicit approval of the Information Custodian (Note: Functional ids may be exempted from this requirement);
- A documented process to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use;
- A process/system to ensure that access privileges are traceable to a unique user id;
- An automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon.

6.4 Audit Trail

The following minimum set of events/actions must be logged and kept as required by State and Federal laws/regulations:

- Additions, changes or deletions to data produced by IT systems;
- Identification and authentication processes;
- Actions performed by system operators, system managers, system engineers, technical support, data security officers, and system administrators;
- Emergency actions performed by support personnel and highly privileged system and security resources.

The audit trails must include at least the following information:

- Date and time of event;
- User id of person performing the action;
- Type of event;
- Asset or resource name and type of access;
- Success or failure of event;
- Source (terminal, port, location, and so forth) where technically feasible.

6.5 Violation Log Management and Review

The Information Custodian must review all violations within one business day of a discovered occurrence. Automated tools are recommended when performing this review whenever possible. At a minimum the following events should be reviewed:

- Two (2) or more failed attempts per system day to access or modify security files, password tables or security devices;
- Disabled logging or attempts to disable logging;
- Two (2) or more failed attempts to access or modify nonpublic information within a week;
- Any unauthorized attempts to modify software or to disable hardware configurations.

Section: 7	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

7 Network Security Standard

Agencies must ensure that all information networks are protected from unauthorized access at all entry points. To help accomplish this, each agency must, at a minimum:

- Establish a process to protect from unauthorized dial-in access;
- Utilize the State approved banner text (See 7.2);
- Establish a process to ensure that all external IP connections are made through a firewall;
- Implement and monitor an Intrusion Detection Systems (IDS) or Intrusion Prevention System (IPS). Automated logging and reporting of this information should be 24x7x365;
- Establish a process to ensure that all Service Interface Agreements (SIAs) are managed in accordance with their IT Security Program and the State Policy;
- Establish a process to ensure that the same level of controls that exist on-site exist for users working remotely;
- Establish a process to prevent unauthorized mobile code from being loaded onto State IT equipment;
- Establish a process for ensuring that wireless network connections do not compromise the Agency's network;
- Establish a process for securing all Private Branch Exchanges (PBXs);
- Establish a process to prevent unauthorized networks to access VoIP networks.

7.1 Dial-in Access

The following services are prohibited except where they are specifically approved by the Agency CIT:

- Dial-in desktop modems;
- Use of any type of "remote control" product (e.g., PCAnywhere, GoToMyPC);
- Use of any network-monitoring tool.

In addition, the following controls for dial-in users must be implemented:

- Unique network access user ids different from their application or network user id;
- A minimum prohibition of answer or pickup until after the sixth (6th) ring;
- Access privileges must be prohibited to any applications except those expressly required (i.e. cannot grant access to entire network, must be application specific);
- Annual review of access requirements;
- Shall not store data unless the data can be protected from unauthorized access, modification, or destruction.

7.2 Banner Text

The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs:

"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of

Maryland and may be used by the State of Maryland for any purpose.”

An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read. The banner is:

- Required for all mainframe, midrange, workstation, personal computer, and network systems;
- Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices;
- The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen. In such cases, this negative impact must be documented in the Agency’s IT Security Program.

7.3 Firewalls & Network Devices

State networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. State firewalls should be configured to block all services not required, disable unused ports, hide and prevent direct access to State trusted network addresses from untrusted networks, prevent access by unauthorized source IP addresses or subnets, maintain comprehensive audit trails, fail in a closed state and operate on a dedicated platform (device).

All publicly accessible servers will be placed on a firewall interface configured as a DMZ. This DMZ must be separated from any interfaces connected directly to the internal network interface.

All network devices (e.g. servers, routers) shall have all non-needed services disabled and the security for those devices hardened. Publicly managed email and chat services will be prohibited inside an Agency network unless approved by the Agency CIT. All devices shall have updates and patches installed on a timely basis to correct significant security flaws. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

7.4 Intrusion Detection Systems

State networks will be monitored by an IDS or IPS implemented at critical junctures. Host-based, network-based, or a combination of both (preferred) may be utilized. IDS/IPS must be monitored and/or information logged 24x7x365. Each agency must establish a severity and escalation list based upon anticipated events that include immediate response capability when appropriate. These plans should be incorporated in the Agency’s IT Security Program.

7.5 Service Interface Agreement

External network connections shall be permitted only after all approvals are obtained consistent with this policy and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system IT Security Certification and Accreditation package and in the IT System security plan. An SIA shall include:

- Purpose and duration of the connection as stated in the agreement, lease, or contract;
- Points-of-contact and cognizant officials for both the State and non-State organizations;
- Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations;
- Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection;
- Requirements for notifying a specified State official within a specified period of time of a

- security incident on the network, with the recommended time within 4 hours of the incident;
- A provision allowing the State to periodically test the ability to penetrate the non-state network through the external network connection or system.

7.6 Teleworking

In a telecommuting environment, an agency must require the same level of security on the microcomputer used at home or offsite as the microcomputer used in the workplace.

7.7 Mobile Code

Until reliable executable content scanning technology is available to address security concerns with regard to mobile code or executables obtained via the Web, all mobile code or executable content employed within a agency intranet shall be documented in the IT System Security Plan and approved by the Agency CIT.

7.8 Wireless Networks

7.8.1 General Controls

Each agency must:

- Complete a Certification and Accreditation of the wireless system before production implementation including the creation of a Wireless Security Plan (Reference <http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf> for guidance);
- Maintain a current, documented diagram of the topology of the wireless network;
- Label and keep an inventory of the wireless and handheld devices;
- Perform periodic security testing and assessment of the wireless network;
- Perform ongoing, randomly timed security audits to monitor and track wireless laptop and handheld PDA usage on the network to ensure only authorized users are utilizing the network;
- Implement configuration/change control and management to ensure that equipment has the latest software release that includes security enhancements and patches for discovered vulnerabilities;
- Implement standardized configuration to reflect the Wireless Security Plan, to ensure change of default values, and to ensure consistency of operation;
- Implement security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies;
- Monitor the wireless industry for changes to standards that enhance security features and for the release on new products;
- Vigilantly monitor wireless technology for new threats and vulnerabilities;
- Wireless networks must implement some form of cryptographic protocol, examples being secure shell (SSH), Transport-Level Security (TLS), Internet Protocol Security (IPsec), or Virtual Private Networks (VPN);
- Additional countermeasures such as strategically locating access points, ensuring firewall filtering, blocking, and the installation of antivirus software must be implemented.

7.8.2 Wireless Security Plan

The Wireless Security Plan must do the following:

- Identify who may use the technology in the agency;

- Identify whether Internet access is required;
- Describe who can install access points and other wireless equipment;
- Provide limitation on the location of and physical security for access points;
- Describe the type of information that may be sent over wireless links;
- Describe the conditions under which wireless devices are allowed;
- Define standard security settings for access points;
- Describe limitation on how the wireless devices may be used;
- Describe the hardware and software configuration of all wireless devices;
- Provide guidelines on reporting losses of wireless devices and security incidents;
- Provide guidelines for the protection of wireless clients to minimize/reduce theft;
- Define the frequency and scope of security assessments to include access point discovery.

Access Point Configuration

- All default passwords must be changed to comply with the State of Maryland password policies before production implementation;
- The Secure Set Identifier (SSID) must be changed from the factory default before production implementation;
- The beacon interval which announces the existence of a wireless network should be set to its highest value;
- Disable the broadcast SSID feature;
- Change default cryptographic keys;
- If SNMP is not required, the agency should disable it;
- If SNMP is required, agencies must use SMNPv3 or higher;
- Dynamic Host Control Protocol (DHCP) should be disabled and static IP addresses should be used on the wireless network, if feasible, and/or utilize access points with integrated firewalls.

Authentication

- The access point must verify the identity of the wireless device (i.e., open-system authentication and WEP and WEP2 are prohibited).

Intrusion Detection/Prevention Systems

- Host Based Intrusion Detection System (IDS) or Intrusion Prevention Systems (IPS) must be implemented on the wireless network wherever possible.

7.9 Private Branch Exchange (PBX)

If PBX processors require remote vendor maintenance via a dial-in telephone line the following controls must be in place:

- A single dedicated telephone line that disables access to the public-switched telephone network;
- An automated audit trail;
- Encryption of transmissions;
- Access controls.

7.10 Facsimile

Data transmitted by facsimile must be treated in the same manner as any data communicated by network or PBX based on system sensitivity and data classification.

Section: 8	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

8 Physical Security Standard

Physical access to IT information processing, storage areas, and storage devices and its supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas. Agencies must:

- Secure IT areas with controls commensurate to the risks;
- Ensure the secure destruction of storage media;
- Ensure secure media reuse;
- Ensure secure storage of media;
- Obtain personnel security clearances where appropriate.

8.1 Secured IT Areas

Physical access controls must be in place for the following:

- Data Centers;
- Areas containing servers and associated media;
- Networking cabinets and wiring closets;
- Power and emergency backup equipment;
- Operations and control areas.

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be:

- Based on frequency of need for access;
- Approved by the manager responsible for the secured area.

Each agency is responsible for:

- Issuing picture id badges to all Employees/contractors and ensuring that these badges are openly displayed at all times;
- Ensuring that all portable storage media such as hard drives, flash media drives, diskettes, magnetic tapes, laptops, PDA devices, DVDs and CDs are physically secured;
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems;
- Ensuring that any physical access controls are auditable.

8.2 Storage Media Disposal

When no longer usable, diskettes, compact disks, tape cartridges, ribbons, and other similar items shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing (Ref: <http://www.nsa.gov/ia/government/mdg.cfm?MenuID=10.3.1>). No IT equipment shall be released from an agency's control until the equipment is sanitized and all stored information has been cleared. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient. This includes equipment transferred to schools, as well as equipment maintenance and repair.

8.3 Media Reuse

When no longer required for mission or project completion, media (tapes, disks, hard drives, etc.) to be used by another person within the agency shall be overwritten with software and protected consistent with

the data sensitivity of which the IT storage media were previously used. The procedures shall be documented in the IT System Security Plan.

8.4 Storage and Marking

IT Systems and electronic media shall be protected and marked in accordance with the data sensitivity. Users shall not store data on electronic media that cannot be adequately secured against unauthorized access. Data to be electronically transferred to a remote storage location should be transferred only by a secure and encrypted method.

8.5 Personnel

Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

Section: 9	Date Adopted: June 2003	Date Revised: December 2005
------------	-------------------------	-----------------------------

9 Microcomputer/PC/Laptop Security Standard

Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes/stores data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices. To help accomplish this each agency must establish at a minimum the following:

- General controls;
- Virus protection;
- Software licensing and use controls;
- Laptop security and mobile computing controls;
- Protection from personally owned microcomputers and portable storage devices.

9.1 General Controls

All microcomputers that store and/or access nonpublic information must implement the following controls:

User identification and password to control access at logon:

- Encryption to protect directories, sub-directories, and/or files containing nonpublic information;
- Virus Protection.

Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:

- Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing;
- Be updated as soon as updates are available from the vendor;
- Be configured to prevent connection to the network unless the accessing microcomputer has the latest version of the virus product and update installed.

9.2 Software Licenses and Use

Unless specifically approved by the Agency CIT and the agency head, personal or corporate IT equipment shall not have State licensed software installed and shall not be used to process or transmit nonpublic data. Only State owned and authorized computer software is to be used on standalone or networked computer equipment. The State will provide legally acquired software to meet legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.

Authorized software packages are those approved by the Agency CIT. Executable modules cannot be downloaded from the Internet unless authorized by the Agency CIT and agency network administrator. Agencies should designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

9.3 Laptop Security and Mobile Computing

Laptops and mobile computing devices are not authorized to process or store nonpublic information unless approved in writing by the agency network support administrator, the Agency CIT and the agency head. Laptops and mobile computing devices which include personal digital assistants approved for

processing nonpublic information cannot be connected to State networks or systems unless the network or system is certified and accredited for that function. In such cases the IT Security Program will identify the devices that can be used to access the network or the system, the purposes for the access, and the security controls for the connection.

9.4 Personally Owned Data Processing Equipment

Personal or contractor owned data processing and data storage equipment (i.e., not owned by the State) are prohibited from accessing systems with nonpublic information and processing or storing nonpublic information unless approved by the agency network support administrator and the Agency CIT.

Section: 10	Date Adopted: June 2003	Date Revised: December 2005
-------------	-------------------------	-----------------------------

10 Encryption Standard

Agencies must ensure that encryption is utilized to protect any nonpublic information when it is stored or transmitted through any environment. IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (Reference <http://csrc.nist.gov/publications/fips/> for guidance).

To help accomplish this each agency using encryption must establish at a minimum the following:

- Secure cryptographic keys;
- Use of Public Key Cryptography methods approved by the State CIT;
- All cryptographic keys must have a designated, unique owner.

Key change intervals shall be established by each agency, but must be no longer than the following:

- Master keys must be changed once per year, if the product allows;
- Key encrypting keys (e.g., asymmetric encrypting a symmetric) must be changed at a minimum of every six (6) months;
- Link encrypting keys must be changed every six (6) months.

Keys must be distributed in a secure manner ensuring that the entire key is not exposed while in transit to any one individual at any one time.

Default cryptographic keys may not be utilized. Exceptions are for emergency recovery, system calibration or vendor certification purposes. In such cases, a documented process describing the storage, maintenance, use and destruction of these keys must be in place.

10.1 Public Key Technology (Asymmetric)

All public key management systems, Certificate Authorities (CAs), key distribution systems, key recovery systems, and cross-certification processes must be approved by the State CIT. Every public key and certificate must have an associated scope of use, which must be checked by any user or server that accepts or relies upon the certificate.

The process for issuing digital certificates must:

- Establish the identity of the subject;
- Establish that the subject is the holder of the associated private keys;

Section: 11	Date Adopted: June 2003	Date Revised: December 2005
-------------	-------------------------	-----------------------------

11 IT Information Security Deviation/Risk Acceptance Standard

An Information Security Deviation Request/Risk Acceptance form must be completed by the agency if it determines that it cannot or will not comply with the State IT Security Policy. All deviation requests require the approval of the agency CIT, agency head, and the State CIT.

11.1 General Requirements

- Proposed deviations will be considered on an individual basis;
- Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures and extenuating circumstances associated with the proposed deviation and its impact on IT systems;
- Requests for deviations must be made in writing;
- Deviations will be granted for a maximum period of twelve (12) months after which time the deviation will be considered expired and require renewal.

Section: 12	Date Adopted: June 2003	Date Revised: December 2005
-------------	-------------------------	-----------------------------

12 Use of Electronic Communications Standard

This standard applies to information technology security, however, it is not inclusive of other State policies and regulations that may further apply to the use of electronic communications.

The use of the Internet, E-mail and other State computing equipment, networks and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. Information communicated electronically through email, the Internet or sharing of electronic documents is subject to State laws, regulations, policies and other requirements, as is information communicated in other written forms and formats. Access to State agency email or Internet services may be wholly or partially restricted without prior notice and without user consent.

12.1 Internet and Electronic Communications

Users accessing the Internet or other State electronic communications through State resources may be monitored. Agencies shall develop standards consistent with all State policies and standards regarding E-mail, Internet use, and use of other computer resources. Electronic communications that are not secure or encrypted should not be used to send information that is nonpublic information.

12.2 Computer Software and Copyright Infringement

The State will not permit the making or using of unauthorized software copies under any circumstances. This includes, but is not limited to programs; executable modules and screen savers (e.g. downloaded software, pirated software, software not licensed to the State, software brought from home). Agencies will establish and enforce internal controls to prevent the making or use of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards. For additional guidance refer to Annotated Code of Maryland, Criminal Law, Section 7-302.

The Agency CIT is responsible for ensuring that the agency is abiding by the terms of all software licenses and for compliance with the prevention of software copyright infringement and protection. The Agency CIT, or designee, shall establish and maintain positive control of software, including inventory measures and accounting procedures that document all purchases of software. Each agency shall establish written procedures that include at a minimum the following:

- Control of all software and software licenses;
- A program that informs employees about the need to comply with software licenses;
- Requirement for all employees to sign the State of Maryland Software Code of Ethics (Attachment 1).

12.3 IT Incident and Advisories

Each agency shall notify its staff of the personnel designated to provide authenticated notices of IT incidents and advisories. Employees other than the designated personnel shall not forward IT Incident advisories to agency staff. If an advisory comes to an employee, the employee shall forward it to the designated personnel for evaluation.

13 Record of Revisions

Issue	Date	Section	Description
Revision 1.5	January 2007	All	Minor formatting changes
Revision 1.4	December 2006	All	Annual review and validation of content.
Revision 1.3	December 2005	Cover Page	Modified date and revision
		1	Changed Format
		1.1, 1.4	Removed reference to Executive Order
		1.6	Added language: guidance and reference
		2	Changes format, added terms and definitions: IPS, Untrusted Network, VoIP
		3	Changed format
		3.1	Added Enforcing State security policy
		4	Changed format
		4.9	Removed reference to State Data Security Committee
		6	Removed bullet line 6
		6.1.1	Changed bullet line 9 to reflect 90 days for general users. Changed line 11 to allow for a 10 minute automatic reset
		6.2	Changed bullet line 5: removed the 90 removal reference
		7	Changed format, added VoIP
		7.4	Added Intrusion Prevention System
		7.8	Added language: guidance. Added IPS reference
		8	Changed format
		8.2	Removed reference to second URL "Miami.edu"
		8.4	Added reference to secure and encrypted method.
		9	Changed format
		9	Added "processes/stores"
		9.2	Removed reference to DBM

Issue	Date	Section	Description
		10	Changed format, changed language to state “reference”, “guidance”.
		11	Changed format
		12	Changed format
		12.2	Changed heading, added paragraph to cover SCOE position.
		13 (old)	Removed
		14	Changed to Section 13
			Added Revision references for 2005
		14	Appended Software Code of Ethics attachment
Revision 1.2	December 2004	1.7	Agency deviation approval list modified
		2	Mobile Code definition added, Nonpublic Definition added, PPI Definition removed and all references to PPI changed to nonpublic.
		7.8	Wireless Network Controls, Security Plan, A.P. Configuration, Authentication, IDS.
		8.2	Storage Media Disposal
		9.4	Personally Owned Data Processing Equipment.
		11.1	Requests for deviations format
Revision 1.1	July 24, 2003	7.2	Banner Text modified.
Policy issued	June 6, 2003	N/A	N/A

ATTACHMENT 1

STATE OF MARYLAND

SOFTWARE CODE OF ETHICS

Unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct. The State disapproves of such copying and recognizes the following principles as a basis for preventing its occurrence.

1. The State will not permit the making or using of unauthorized software copies under any circumstances.
2. The State will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.
3. The State will enforce internal controls to prevent the making or using of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards.

My signature indicates that I have read and understand this State of Maryland Software Code of Ethics. I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making or using unauthorized software may also subject me to civil and criminal penalties.

SIGNATURE: _____ DATE: _____

NAME: (Please Print): _____

AGENCY: _____

DIVISION: _____

LOCATION: _____

**State of Maryland
Comptroller of Maryland**

Vendor Electronic Funds Transfer (EFT) Registration Request Form

Date of request _____

Business identification information (Address to be used in case of default to check):

Business Name _____

Address line 1 _____

Address line 2 _____

City _____ State _____ Zip code _____

Business taxpayer identification number: _____

Federal Employer Identification Number: _____

(or) Social Security Number: _____

Business contact name, title, and phone number including area code. (And address if different from above).

Financial institution information:

Name and address _____

Contact name and phone number (include area code) _____

ABA number: _____

Account number: _____

Account type: Checking/ Money / Market

A VOIDED CHECK from the bank account must be attached.

Transaction requested:

1. ___ Initiate all disbursements via EFT to the above account.
2. ___ Discontinue disbursements via EFT, effective _____
3. ___ Change the bank account to above information – a copy of the approved Registration Form for the previous bank account must be attached.

I am authorized by

* _____ (hereinafter Company) to make the representations contained in this paragraph. Company authorizes the Comptroller and the Treasurer of Maryland to register it for electronic funds transfer (EFT) using the information contained in this registration form. Company agrees to receive all funds from the State of Maryland by electronic funds transfer according to the terms of the EFT program. Company agrees to return to the State of Maryland any EFT payment incorrectly disbursed by the State of Maryland to the Company's account. Company agrees to hold harmless the State of Maryland and its agencies and departments for any delays or errors caused by inaccurate or outdated registration information or by the financial institution listed above.

*Name of registering business entity

Signature of company treasurer, controller, or chief financial officer and date

Completed by GAD/STO

Date Received _____
GAD registration information verified _____ Date to STO _____
STO registration information verified _____ Date to GAD _____
R*STARS Vendor No. and Mail Code Assigned:

_____/_____/_____

State Treasurer's Office Approval Date

General Accounting Division Approval Date

Requestor:

Please retain a copy of this form for your records. Please allow approximately 30 days from the date of your request for the Comptroller's and Treasurer's Offices to process your request. Failure to maintain current information with this office could result in errors in payment processing. If you have any questions, please call the EFT registration desk at 410-260-7375.

Please submit form to:

EFT Registration, General Accounting Division
Room 205, P.O. Box 746
Annapolis, Maryland 21404-0746

COT/GAD X-10

Living Wage Requirements for Service Contracts

- A. This contract is subject to the Living Wage requirements under Title 18, State Finance and Procurement Article, Annotated Code of Maryland and the regulations proposed by the Commissioner of Labor and Industry. The Living Wage generally applies to a Contractor or Subcontractor who performs work on a State contract for services that is valued at \$100,000 or more. An employee is subject to the Living Wage if he/she is at least 18 years old or will turn 18 during the duration of the contract; works at least 13 consecutive weeks on the State Contract and spends at least one-half of the employee's time during any work week on the State Contract.
- B. The Living Wage Law does not apply to:
 - (1) A Contractor who:
 - (A) has a State contract for services valued at less than \$100,000, or
 - (B) employs 10 or fewer employees and has a State contract for services valued at less than \$500,000.
 - (2) A Subcontractor who:
 - (A) performs work on a State contract for services valued at less than \$100,000,
 - (B) employs 10 or fewer employees and performs work on a State contract for services valued at less than \$500,000, or
 - (C) performs work for a contractor not covered by the Living Wage Law as defined in B(1)(B) above, or B (3) or C below.
 - (3) Service contracts for the following:
 - (A) services with a Public Service Company;
 - (B) services with a nonprofit organization;
 - (C) services with an officer or other entity that is in the Executive Branch of the State government and is authorized by law to enter into a procurement ("Unit"); or
 - (D) services between a Unit and a County or Baltimore City.

- C. If the Unit responsible for the State contract for services determines that application of the Living Wage would conflict with any applicable Federal program, the Living Wage does not apply to the contract or program.
- D. A Contractor must not split or subdivide a State contract for services, pay an employee through a third party, or treat an employee as an independent contractor or assign work to employees to avoid the imposition of any of the requirements of Title 18, State Finance and Procurement, Annotated Code of Maryland.
- E. Each Contractor/Subcontractor, subject to the Living Wage Law, shall post in a prominent and easily accessible place at the work site(s) of covered employees a notice of the Living Wage Rates, employee rights under the law, and the name, address, and telephone number of the Commissioner.
- F. The Commissioner of Labor and Industry shall adjust the wage rates by the annual average increase or decrease, if any, in the Consumer Price Index for all urban consumers for the Washington/Baltimore metropolitan area, or any successor index, for the previous calendar year, not later than 90 days after the start of each fiscal year. The Commissioner shall publish any adjustments to the wage rates on the Division of Labor and Industry's Website. An employer subject to the Living Wage Law must comply with the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate, required by the Commissioner, automatically upon the effective date of the revised wage rate.
- G. A Contractor/Subcontractor who reduces the wages paid to an employee based on the employer's share of the health insurance premium, as provided in §18-103(c), State Finance and Procurement Article, Annotated Code of Maryland, shall not lower an employee's wage rate below the minimum wage as set in §3-413, Labor and Employment Article, Annotated Code of Maryland. A Contractor/Subcontractor who reduces the wages paid to an employee based on the employer's share of health insurance premium shall comply with any record reporting requirements established by the Commissioner of Labor and Industry.
- H. A Contractor/Subcontractor may reduce the wage rates paid under §18-103(a), State Finance and Procurement, Annotated Code of Maryland, by no more than 50 cents of the hourly cost of the employer's contribution to an employee's deferred compensation plan. A Contractor/Subcontractor who reduces the wages paid to an employee based on the employer's contribution to an employee's deferred compensation plan shall not lower the employee's wage rate below the minimum wage as set in §3-413, Labor and Employment Article, Annotated Code of Maryland.

- I. Under Title 18, State and Finance Procurement Article, Annotated Code of Maryland, if the Commissioner determines that the Contractor/Subcontractor violated a provision of this title or regulations of the Commissioner, the Contractor/Subcontractor shall pay restitution to each affected employee, and the State may assess liquidated damages of \$20 per day for each employee paid less than the Living Wage.
- J. Information pertaining to reporting obligations may be found by going to the DLLR Website <http://www.dlfr.state.md.us/> and clicking on Living Wage.

Affidavit of Agreement
Maryland Living Wage Requirements-Service Contracts

Re: Solicitation No. _____

Offer/Bid submitted by (name of firm)_____

Address_____

City_____ State_____ Zip Code_____

The Undersigned, being an authorized representative of the above stated Bidder/Offeror, hereby affirms our commitment to comply with Title 18, State Finance and Procurement Article, Annotated Code of Maryland and to submit all payroll reports to the Commissioner of Labor and Industry with regard to the above stated contract.

The Bidder/Offeror agrees to pay employees who are subject to living wage at least the living wage rate in effect at the time service is provided for hours spent on State contract activities, and to ensure that its Subcontractors who are not exempt also pay the required living wage rate to their employees who are subject to the living wage for hours spent on a State contract for services. The Bidder/Offeror agrees to comply with, and ensure its Subcontractors comply with, the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate established by the Commissioner of Labor and Industry, automatically upon the effective date of the revised wage rate.

(If applicable) The Bidder/Offeror provides the following reasons why the affirmations above cannot be given and affirms that it is exempt from Maryland's Living Wage Law for the following reasons:_____

Name of Authorized Representative: _____

Signature of Authorized Representative Date

Title

Witness Name (Typed or Printed)

Witness Signature Date

