

**CONTRACT #5**  
**RFS # 344.01-00420**  
**Edison # 35033**

**Department of Intellectual and  
Developmental Disabilities**

**VENDOR:**  
**Mid-America Consulting Group,  
Inc.**



STATE OF TENNESSEE  
**DEPARTMENT OF INTELLECTUAL AND DEVELOPMENTAL DISABILITIES**  
CITIZENS PLAZA BUILDING  
400 DEADERICK STREET, 10<sup>th</sup> Floor  
NASHVILLE, TENNESSEE 37243

September 5, 2014

Mr. Lucian Geise, Executive Director  
Fiscal Review Committee  
8th Floor, Rachel Jackson Building  
320 Sixth Avenue, North  
Nashville, Tennessee 37243

ATTENTION: Leni Chick

RE: Request for Contract Amendment Review  
Mid-America Consulting Group, Inc., Edison Record ID # 35033  
Contract Services for Configuration and Implementation of the Microsoft Dynamics HHS Platform

Dear Mr. Geise:

The Department of Intellectual and Developmental Disabilities (DIDD) is submitting proposed Amendment 1 to Edison Record ID # 35033 with Mid-America Consulting Group, Inc. for review in accordance with TCA, Section 4-56-107 (b)(1)(B).

DIDD is proposing an amendment to the contract to extend the contract term and to revise contract payment methodology. All phases of the scope of services will not be complete by the current ending date of 11/17/2014 and DIDD needs to revise the payment methodology to clarify rendering payment to the vendor for completed services at the time of their delivery of work.

The proposed amendment and Non-Competitive Amendment Request is enclosed along with a copy of the base contract, completed *"Supplemental Documentation Required for Fiscal Review Committee"* form, pre-approved OIR Endorsement Request, and spreadsheets of expenditures and anticipated expenditures under this contract through the proposed ending date of June 30, 2016.

Please let me know if any additional information is required for review of this request. Your assistance for review of this proposed amendment is appreciated.

Sincerely,

A handwritten signature in black ink that reads "Debra K. Payne".

Debra K. Payne  
Commissioner

DKP:LI:DD

Enclosures

Supplemental Documentation Required for  
Fiscal Review Committee

*Contact Name:	Lance D. Iverson Deputy Commissioner of Fiscal and Administration	*Contact Phone:	253-6710		
*Presenter's name(s):	Lance D. Iverson Deputy Commissioner of Fiscal and Administration <a href="mailto:Lance.D.Iverson@tn.gov">Lance.D.Iverson@tn.gov</a> 253-6710  Russell Nicoll Chief Information Officer <a href="mailto:Russell.Nicoll@tn.gov">Russell.Nicoll@tn.gov</a> 741-6632				
Edison Contract Number: <i>(if applicable)</i>	35033	RFS Number: <i>(if applicable)</i>	34401-00420		
*Original or Proposed Contract Begin Date:	11/17/2012	*Current or Proposed End Date:	11/16/2014		
Current Request Amendment Number: <i>(if applicable)</i>	1				
Proposed Amendment Effective Date: <i>(if applicable)</i>	11/17/2014				
*Department Submitting:	Department of Intellectual and Developmental Disabilities				
*Division:	Administration				
*Date Submitted:	9/8/2014				
*Submitted Within Sixty (60) days: <i>If not, explain:</i>	Yes N/A				
*Contract Vendor Name:	Mid-America Consulting Group, Inc.				
*Current or Proposed Maximum Liability:	\$1,286,560.00				
*Estimated Total Spend for Commodities:	N/A				
<b>*Current or Proposed Contract Allocation by Fiscal Year: (as Shown on Most Current Fully Executed Contract Summary Sheet)</b>					
FY: 2013	FY: 2014	FY: 2015	FY: 2016	FY:	FY:
\$ 233,920	\$ 643,280	\$ 292,400	\$ 116,960	\$	\$
<b>*Current Total Expenditures by Fiscal Year of Contract: (attach backup documentation from Edison)</b>					
FY: 2013	FY: 2014	FY: 2015	FY: 2016	FY:	FY:
\$ 0.00	\$ 311,893.00	\$ 740,747.00	\$ 233,920.00	\$	\$
IF Contract Allocation has been greater than Contract			N/A		

Supplemental Documentation Required for  
Fiscal Review Committee

Expenditures, please give the reasons and explain where surplus funds were spent:			
IF surplus funds have been carried forward, please give the reasons and provide the authority for the carry forward provision:		N/A	
IF Contract Expenditures exceeded Contract Allocation, please give the reasons and explain how funding was acquired to pay the overage:		N/A	
*Contract Funding Source/Amount:			
State:		Federal:	
<i>Interdepartmental:</i>	\$1,286,560.00	<i>Other:</i>	
If “ <i>other</i> ” please define:		N/A	
If “ <i>interdepartmental</i> ” please define:		Bureau of TennCare – Intellectual Disabilities Services (318.71)	
Dates of All Previous Amendments or Revisions: <i>(if applicable)</i>		Brief Description of Actions in Previous Amendments or Revisions: <i>(if applicable)</i>	
N/A		N/A	
Method of Original Award: <i>(if applicable)</i>		RFP	
*What were the projected costs of the service for the entire term of the contract prior to contract award? How was this cost determined?		The projected expenditures associated with implementation services prior to contract award was \$1,800,000. This projection was assumed as the remaining available funds as part of a \$10,100,000 overall budget for Project Titan as originally appropriated in 2008 Public Chapter 1203, Section 48, Item 11.	
*List number of other potential vendors who could provide this good or service; efforts to identify other competitive procurement alternatives; and the reason(s) a sole-source contract is in the best interest of the State.		N/A	



**Payments and Anticipated Expenditures  
Mid-America Consulting Group, Inc.  
Edison Record ID 35033**

**Payments made to date:**

<b>Payment Amount</b>	<b>Payment Date</b>	<b>FY</b>	<b>Service Description</b>
\$210,528.00	09/13	FY 2014	Design Document
\$23,392.00	10/13	FY 2014	Design Document (withheld)
\$77,973.00	06/13	FY 2014	Phase 1A (Wait List)
<b>\$311,893.00</b>	<b>Total Paid Fiscal Year 2014</b>		

**Anticipated Expenditures:**

<b>Payment Amount</b>	<b>Payment Date</b>	<b>FY</b>	<b>Service Description</b>
\$58,480.00		FY2015	Detailed Design
\$155,947.00		FY2015	Phase 1A (Service Planning)
\$70,176.00		FY2015	Phase 1 Ownership
\$175,440.00		FY2015	Phase 3 (Protection from Harm)
\$52,632.00		FY2015	Phase 3 Ownership
\$175,440.00		FY2015	Phase 2 (Service Tracking)
\$52,632.00		FY2015	Phase 2 Ownership
<b>\$740,747.00</b>	<b>Total Budgeted Fiscal Year 2015</b>		

<b>Payment Amount</b>	<b>Payment Date</b>	<b>FY</b>	<b>Service Description</b>
\$46,784.00		FY2016	Phase 1 Warranty
\$35,088.00		FY2016	Phase 2 Warranty
\$35,088.00		FY2016	Phase 3 Warranty
\$116,960.00		FY2016	Change Orders
<b>\$233,920.00</b>	<b>Total Budgeted Fiscal Year 2016</b>		

<b>\$1,286,560.00</b>	<b>Total Contract Amount</b>		
-----------------------	------------------------------	--	--

# Amendment Request

Route a completed request, as one file in PDF format, via e-mail attachment sent to: [Agsprrs.Agsprsr@tn.gov](mailto:Agsprrs.Agsprsr@tn.gov)

**APPROVED**

CHIEF PROCUREMENT OFFICER

DATE

<b>Request Tracking #</b>	34401-00420	
<b>1. Procuring Agency</b>	Department of Intellectual and Developmental Disabilities	
<b>2. Contractor</b>	Mid-America Consulting Group, Inc.	
<b>3. Contract #</b>	35033	
<b>4. Proposed Amendment #</b>	1	
<b>5. Edison ID #</b>	160152	
<b>6. Contract Begin Date</b>		11/17/2012
<b>7. Current Contract End Date</b> – with ALL options to extend exercised		11/17/2014
<b>8. Proposed Contract End Date</b> – with ALL options to extend exercised		6/30/2016
<b>9. Current Maximum Contract Cost</b> – with ALL options to extend exercised		\$ 1,286,560.00
<b>10. Proposed Maximum Contract Cost</b> – with ALL options to extend exercised		\$ 1,286,560.00
<b>11. Office for Information Resources Pre-Approval Endorsement Request</b> – information technology service (N/A to THDA)	<input type="checkbox"/> Not Applicable	<input checked="" type="checkbox"/> Attached
<b>12. eHealth Pre-Approval Endorsement Request</b> – health-related professional, pharmaceutical, laboratory, or imaging	<input checked="" type="checkbox"/> Not Applicable	<input type="checkbox"/> Attached
<b>13. Human Resources Pre-Approval Endorsement Request</b> – state employee training service	<input checked="" type="checkbox"/> Not Applicable	<input type="checkbox"/> Attached
<b>14. Explanation Need for the Proposed Amendment</b>		
<p>DIDD is proposing an amendment to the contract to extend the contract term and to revise contract payment methodology.</p> <p>All phases of the scope of services will not be complete by the current ending date of 11/17/2014 and DIDD needs to revise the payment methodology to clarify rendering payment to the vendor for completed services at the time of their delivery of work.</p>		

**15. Name & Address of the Contractor's Principal Owner(s)**

– NOT required for a TN state education institution

Johnathan Kaffen  
 Mid-America Consulting Group, Inc.  
 3700 Euclid Ave, Second Floor  
 Cleveland, Ohio 44115  
 Johnathan.Kaffen@mcgcorp.com  
 Telephone # (216) 392-7822 (cell)  
 Telephone # (216) 432-6909 (office)  
 FAX # (216) 432-6925

**16. Evidence Contractor's Experience & Length Of Experience Providing the Goods or Services**

Mid-America Consulting Group, Inc. has been in business for approximately 28 years and has worked with counties and states for design and implementation of web-base tracking and case management automated systems for over 17 years.

**17. Efforts to Identify Reasonable, Competitive, Procurement Alternatives**

This contract was awarded competitively (RFP 34401-00420); however, Mid-America, Inc. was the only proposer in response to the RFP.

**18. Justification**

This contract started on 11/17/2012. DIDD has invested nearly 2 years and \$311,893 in the implementation effort of the Project TITAN solution. DIDD requests extension of the contract term to allow the contractor additional time for completion of the work required for implementation. To let this contract end and start a new procurement process (RFP) to award a new implantation services contract for the completion of the project is not in the best interest of the state considering the efforts made, knowledge learned, successes gained by all parties involved over the past 2 years. DIDD requests adjustment to the payment methodology in order to support the contractor during an extended implantation timeline while retaining incentives for performance and without increasing the maximum liability of the contract.

**Agency Head Signature and Date** – MUST be signed by the ACTUAL agency head as detailed on the current Signature Certification. Signature by an authorized signatory is acceptable only in documented circumstances

 9/8/14



## OIR Pre-Approval Endorsement Request E-Mail Transmittal

**TO :** Jane Chittenden, OIR Contracts  
Department of Finance & Administration  
E-mail: [Jane.Chittenden@tn.gov](mailto:Jane.Chittenden@tn.gov)

**FROM :** Russell Nicoll, Chief Information Officer  
Department of Intellectual & Developmental Disabilities  
Phone: (615) 741-6632

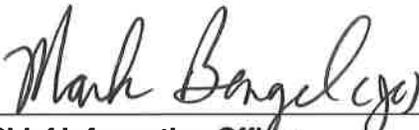
E-mail : [Russell.Nicoll@tn.gov](mailto:Russell.Nicoll@tn.gov)

**DATE :** 9/4/2014

**RE :** Request for OIR Pre-Approval Endorsement

**Applicable RFS#** 34401-00420 / **Edison Record ID** 35033

**OIR Endorsement Signature & Date:**

  
**Chief Information Officer**

9/4/14

*NOTE: Proposed contract/grant support is applicable to the subject IT service technical merit.*

Office for Information Resources (OIR) pre-approval endorsement is required pursuant to procurement regulations pertaining to contracts with information technology as a component of the scope of service. This request seeks to ensure that OIR is aware of and has an opportunity to review the procurement detailed below and in the attached document(s). This requirement applies to any procurement method regardless of dollar amount.

Please indicate OIR endorsement of the described procurement (with the appropriate signature above), and return this document via e-mail at your earliest convenience.

<b>Contracting Agency</b>	<b>Department of Intellectual and Developmental Disabilities</b>
<b>Agency Contact</b> (name, phone, e-mail)	Russell Nicoll, Chief Information Officer Department of Intellectual & Developmental Disabilities Phone: (615) 741-6632 <a href="mailto:Russell.Nicoll@tn.gov">Russell.Nicoll@tn.gov</a>

**Applicable RFS# 34401-00420 / Edison Record ID 35033**

**Attachments Supporting Request**(mark all applicable)

Note: The complete draft procurement document and the applicable documents listed below must accompany this request when submitted to OIR. Special Contract Requests and Amendment Requests without Agency Head signature are acceptable. OIR is aware that these documents will not have CPO signature when submitted with this request.

- Solicitation Document
- Special Contract Request
- Amendment Request
- Proposed Contract/Grant or Amendment
- Original Contract/Grant and Previous Amendments (if any)
- OIR Pre-Approval Endorsement Request

**Information Systems Plan (ISP) Project Applicability**

To avoid delay of OIR pre-approval, the applicability of an ISP project to the procurement must be confirmed with agency IT staff prior to submitting this request to OIR. If necessary, agency IT staff should contact OIR Planning with questions concerning the need for an ISP project.

IT Director/Staff Name Confirming (required): Russell Nicoll, Chief Information Officer

- Applicable – Approved ISP Project#
- Not Applicable (This procurement was approved by OIR)

**Subject Information Technology Service Description**

Provide a brief summary of the information technology services involved. Clearly identify included technologies such as system development/maintenance, security, networking, *etc.* As applicable, identify the contract or solicitation sections related to the IT services.

The contract (Edison 35033) between the Department of Intellectual and Developmental Disabilities and Mid-America Consulting Group, Inc. is for vendor services for configuration and implementation of the Microsoft Dynamics HHS Platform.

The proposed amendment is for extending the contract term and to clarify/revise payment methodology. The scope of services is not amended.



## OIR Pre-Approval Endorsement Request E-Mail Transmittal

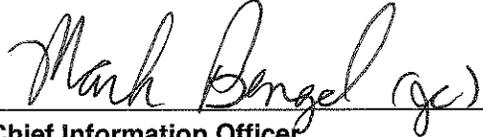
**TO :** Jane Chittenden, OIR Procurement & Contract Management Director  
Department of Finance & Administration  
E-mail : [Jane.Chittenden@tn.gov](mailto:Jane.Chittenden@tn.gov)

**FROM :** Andy Kidd, Sourcing Analyst  
Central Procurement Office  
[andy.kidd@tn.gov](mailto:andy.kidd@tn.gov)

Debra Dunn, Director of Contract Services  
Department of Intellectual and Developmental Disabilities  
[Debra.Dunn@tn.gov](mailto:Debra.Dunn@tn.gov)

**DATE :** 7/12/2012

**RE :** Request for OIR Pre-Approval Endorsement

<b>Applicable RFS #</b>
<b>OIR Endorsement Signature &amp; Date:</b>
 
<b>Chief Information Officer</b>
<i>NOTE: Proposed contract/grant support is applicable to the subject IT service technical merit.</i>

Office for Information Resources (OIR) pre-approval endorsement appears to be required pursuant to professional service contracting regulations pertaining to procurements with information technology as a component of the scope of service. This request seeks to ensure that OIR is aware of and has an opportunity to review the procurement detailed below and in the attached documents.

Please document OIR endorsement of the described procurement (with the appropriate signature above), and return this document via e-mail at your earliest convenience.

<b>Contracting Agency</b>	<b>Department of Intellectual and Developmental Disabilities</b>
<b>Agency Contact</b> (name, phone, e-mail)	Debra Dunn, Director of Contract Services Department of Intellectual and Developmental Disabilities <a href="mailto:Debra.Dunn@tn.gov">Debra.Dunn@tn.gov</a>
<b>Subject Procurement Document</b> (mark one)	

<b>Applicable RFS #</b>	
<input checked="" type="checkbox"/> RFP	<input type="checkbox"/> Contract
<input type="checkbox"/> Competitive Negotiation Request	<input type="checkbox"/> Contract Amendment
<input type="checkbox"/> Alternative Procurement Method Request	<input type="checkbox"/> Grant
<input type="checkbox"/> Non-Competitive Contract Request	<input type="checkbox"/> Grant Amendment
<input type="checkbox"/> Non-Competitive Amendment Request	
<b>Information Systems Plan (ISP) Project Applicability</b>	
<input type="checkbox"/> Not Applicable to this Request	
<input type="checkbox"/> Applicable– ISP Project#	
<b>Response Confirmed by IT Director/Staff</b> (name):	
<b>Required Attachments</b> (as applicable – copies without signatures acceptable)	
<input checked="" type="checkbox"/> RFP, Competitive Negotiation Request, Alternative Procurement Method Request, Non-Competitive Contract Request, Non-Competitive Amendment Request	
<input type="checkbox"/> Original Contract/Grant or Amendment	
<input type="checkbox"/> Proposed Contract/Grant or Amendment	
<b>Subject Information Technology Service Description</b>	
(Brief summary of information technology services involved. Clearly identify included technologies such as system development/maintenance, security, networking, <i>etc.</i> As applicable, identify the contract & solicitation sections related to the IT services.)	
This Request for Proposals is for an implementation service of a product that the DIDD has recently purchased.	
For more information please see:	
<b>RFP # 34401-00420 ATTACHMENT 6.2. — SECTION C</b>	
<b>RFP # 34401-00420 ATTACHMENT 6.6. — SECTION A</b>	



**CONTRACT AMENDMENT COVER SHEET**

<b>Agency Tracking #</b> 34401-00420	<b>Edison ID</b> 35033	<b>Contract #</b> 35033	<b>Amendment #</b> 1		
<b>Contractor Legal Entity Name</b> Mid-America Consulting Group, Inc.			<b>Edison Vendor ID</b> 160152		
<b>Amendment Purpose &amp; Effect(s)</b> Extend Contract Term and Revise Payment Methodology					
<b>Amendment Changes Contract End Date:</b> <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO		<b>End Date:</b> 6/30/2016			
<b>TOTAL Contract Amount INCREASE or DECREASE per this Amendment</b> (zero if N/A):			<b>\$ 0.00</b>		
<b>Funding —</b>					
<b>FY</b>	<b>State</b>	<b>Federal</b>	<b>Interdepartmental</b>	<b>Other</b>	<b>TOTAL Contract Amount</b>
2013			0.00		0.00
2014			\$311,893.00		\$311,893.00
2015			\$740,747.00		\$740,747.00
2016			\$233,920.00		\$233,920.00
<b>TOTAL:</b>			\$1,286,560.00		\$1,286,560.00
<b>American Recovery and Reinvestment Act (ARRA) Funding:</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO					
<b>Budget Officer Confirmation:</b> There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.  Melinda Lanza 253-3166				<i>CPO USE</i>	
<b>Speed Chart</b> (optional)		<b>Account Code</b> (optional)			

**AMENDMENT ONE  
OF CONTRACT 35033**

This Amendment is made and entered by and between the State of Tennessee, Department of Intellectual and Developmental Disabilities, hereinafter referred to as the "State" or "DIDD" and Mid-America Consulting Group, Inc., hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. Contract section B. is deleted in its entirety and replaced with the following:

**B. CONTRACT PERIOD:**

B.1. This Contract shall be effective for the period beginning November 17, 2012, and ending on June 30, 2016. The Contractor hereby acknowledges and affirms that the State shall have no obligation for services rendered by the Contractor which were not performed within this specified contract period.

B.2. Term Extension. The State reserves the right to extend this Contract for an additional period or periods of time representing increments of no more than one (1) year and seven and one half (7½) months and a total contract term of no more than three (3) years and seven and one half (7½) months, provided that such an extension of the contract term is effected prior to the current, contract expiration date by means of a contract amendment. If a term extension necessitates additional funding beyond that which was included in the original Contract, an increase of the State's maximum liability will also be effected through contract amendment, and shall be based upon payment rates provided in the original Contract.

2. Contract section C is deleted in its entirety and replaced with the following:

C.3. Payment Methodology. The Contractor shall be compensated based on the payment rates herein for units of service authorized by the State in a total amount not to exceed the Contract Maximum Liability established in section C.1.

a. The Contractor's compensation shall be contingent upon the satisfactory completion of units, milestones, or increments of service defined in section A.

b. The Contractor shall be compensated for said units, milestones, or increments of service based upon the following payment rates:

Service Description	Amount (per compensable increment)	Percentage of the Total Evaluation Cost Amount
<b>Design Documentation</b>		
Sub-Phase Functional Design Document	\$233,920.00	20.00%
Sub-Phase Detailed Design Document 1	\$19,493.00	1.67%
Sub-Phase Detailed Design Document 2	\$19,493.00	1.67%
Sub-Phase Detailed Design Document 3	\$19,493.00	1.67%

Service Description	Amount (per compensable increment)	Percentage of the Total Evaluation Cost Amount
<b>Phase 1 - Planning</b>		
Sub-Phase 1(A) Intake and Wait List	\$77,973.00	6.67%
Sub-Phase 1(B) Acceptance of Releases 1, 2, and 3	\$71,476.00	6.10%
Sub-Phase 1(B) Acceptance of Release 4	\$42,457.00	3.63%
Sub-Phase 1(B) Acceptance of Release 5	\$100,495.00	8.59%
Total Ownership - Phase 1	\$70,176.00	6.00%
Warranty Period - 1 Year	\$46,784.00	4.00%
<b>Phase 2 - Tracking and Billing</b>		
Sub-Phase - T&B Implementation*	\$40,936.00	3.50%
Sub-Phase - T&B Acceptance	\$76,024.00	6.50%
Total Ownership - Phase 2	\$52,632.00	4.50%
Warranty Period - 1 Year	\$35,088.00	3.00%
<b>Phase 3 - Protection from Harm</b>		
Sub-Phase - PFH Implementation*	\$61,404.00	5.25%
Sub-Phase - PFH Acceptance	\$114,036.00	9.75%
Total Ownership - Phase 3	\$52,632.00	4.50%
Warranty Period - 1 Year	\$35,088.00	3.00%
<b>Total</b>	\$ 1,169,600.00	100.00%
<p>* Implementation: contract term for completion of a phase and "Go Live" agreed upon by State of Tennessee Project Manager or 30 days after delivery of code as indicated on the agreed upon project plan.</p>		

- c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A.1.3., without a formal amendment of this contract based upon the payment rates detailed in the schedule below and as agreed pursuant to said Section A.1.3., PROVIDED THAT compensation to the Contractor for such "change order" work shall not exceed ten percent (10 %) of the sum of milestone payment rates detailed in Section C.3.b., above (which is the total cost for the milestones and associated deliverables set forth in Contract

Sections A.1.2.3., through A.1.2.7.). If, at any point during the Contract period, the State determines that the cost of necessary “change order” work would exceed said maximum amount, the State may amend this Contract to address the need.

<p align="center"><b>Service Description</b> <b>CHANGE ORDER WORK</b></p>	<p align="center"><b>Amount</b> (per compensable increment)</p>
PM (MCG)	\$ 225.00 per hour
BA1	\$ 195.00 per hour
BA2	\$ 195.00 per hour
Architect	\$ 250.00 per hour
Dev 1	\$ 185.00 per hour
Dev 2	\$ 185.00 per hour
Train Lead (Tanner)	\$ 180.00 per hour
Tran2 (Tanner)	\$ 155.00 per hour
UI Dev	\$ 115.00 per hour

d. The Contractor shall not be compensated for travel time to the primary location of service provision.

3. Contract section E.2. is deleted in its entirety and replaced with the following:

E.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by EMAIL or facsimile transmission with recipient confirmation. Any such communications, regardless of method of transmission, shall be addressed to the respective party at the appropriate mailing address, facsimile number, or EMAIL address as set forth below or to that of such other party or address, as may be hereafter specified by written notice.

The State:

Russell Nicoll, Chief Information Officer  
 Department of Intellectual and Developmental Disabilities  
 Citizens Plaza State Office Building  
 400 Deaderick Street, 9<sup>th</sup> Floor  
 Nashville, Tennessee 37243  
 Russell.Nicoll@tn.gov  
 Telephone (615) 741-6632  
 FAX (615) 391-9841

The Contractor:

Johnathan Kaffen  
 Mid-America Consulting Group, Inc.  
 3700 Euclid Ave, Second Floor  
 Cleveland, Ohio 44115

Johnathan.Kaffen@mcgcorp.com  
Telephone # (216) 392-7822 (cell)  
Telephone # (216) 432-6909 (office)  
FAX # (216) 432-6925

All instructions, notices, consents, demands, or other communications shall be considered effectively given upon receipt or recipient confirmation as may be required.

4. The following is added as Contract section E.15.

E.15. Tennessee Department of Revenue Registration. The Contractor shall be registered with the Department of Revenue for the collection of Tennessee sales and use tax. This registration requirement is a material requirement of this Contract.

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective November 5, 2014. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

**IN WITNESS WHEREOF,**

**MID-AMERICA CONSULTING GROUP, INC.:**

---

**SIGNATURE**

**DATE**

---

**PRINTED NAME AND TITLE OF SIGNATORY (above)**

**DEPARTMENT OF INTELLECTUAL AND DEVELOPMENTAL DISABILITIES:**

---

**DEBRA K. PAYNE, COMMISSIONER**

**DATE**



# CONTRACT

(fee-for-service contract with an individual, business, non-profit, or governmental entity of another state)

<b>Begin Date</b> 11/17/2012	<b>End Date</b> 11/16/2014	<b>Agency Tracking #</b> 34401-00420	<b>Edison Record ID</b> 35033
<b>Contractor Legal Entity Name</b> MID-AMERICA CONSULTING GROUP, INC.			<b>Edison Vendor ID</b> 160152

**Service Caption (one line only)**  
VENDOR SERVICES FOR THE CONFIGURATION AND IMPLEMENTATION OF THE MICROSOFT DYNAMICS HHS PLATFORM

<b>Subrecipient or Vendor</b> <input type="checkbox"/> Subrecipient <input checked="" type="checkbox"/> Vendor	<b>CFDA #</b>
---	---------------

Funding					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2013			\$233,920.00		\$233,920.00
2014			\$643,280.00		\$643,280.00
2015			\$292,400.00		\$292,400.00
2016			\$116,960.00		\$116,960.00
<b>TOTAL:</b>			<b>\$1,286,560.00</b>		<b>\$1,286,560.00</b>

**American Recovery and Reinvestment Act (ARRA) Funding:**  YES  NO

**Ownership/Control**

African American   
 Asian   
 Hispanic   
 Native American   
 Female  
 Person w/Disability   
 Small Business   
 Government   
 NOT Minority/Disadvantaged  
 Other:

**Selection Method & Process Summary (mark the correct response to confirm the associated summary)**

<input checked="" type="checkbox"/> RFP	The procurement process was completed in accordance with the approved RFP document and associated regulations.
<input type="checkbox"/> Competitive Negotiation	The predefined, competitive, impartial, negotiation process was completed in accordance with the associated, approved procedures and evaluation criteria.
<input type="checkbox"/> Alternative Competitive Method	The predefined, competitive, impartial, procurement process was completed in accordance with the associated, approved procedures and evaluation criteria.
<input type="checkbox"/> Non-Competitive Negotiation	The non-competitive contractor selection was completed as approved, and the procurement process included a negotiation of best possible terms & price.
<input type="checkbox"/> Other	The contractor selection was directed by law, court order, settlement agreement, or resulted from the state making the same agreement with <u>all</u> interested parties or <u>all</u> parties in a predetermined "class."

<b>Budget Officer Confirmation:</b> There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations. <i>Melinda Lanza 12/3/12</i> Melinda Lanza 253-3166	<b>OCR USE - FA</b>
---	---------------------

<b>Speed Chart (optional)</b>	<b>Account Code (optional)</b>
-------------------------------	--------------------------------

<b>Dept ID</b> 3440100001	<b>Account</b> 70899000	<b>Location CF</b> 19049	<b>Program</b> 344110	<b>User Code</b> 700043
------------------------------	----------------------------	-----------------------------	--------------------------	----------------------------



**CONTRACT  
BETWEEN THE STATE OF TENNESSEE,  
DEPARTMENT OF INTELLECTUAL AND DEVELOPMENTAL DISABILITIES  
AND  
MID-AMERICA CONSULTING GROUP, INC.**

This Contract, by and between the State of Tennessee Department of Intellectual and Developmental Disabilities, hereinafter referred to as the "State" or "DIDD" and Mid-America Consulting Group, Inc., hereinafter referred to as the "Contractor," is for the provision of Configuration and Implementation of The Microsoft Dynamics HHS Platform, as further defined in the "SCOPE OF SERVICES."

The Contractor is a for-profit corporation.  
Contractor Place of Incorporation or Organization: Ohio  
Contractor Edison Registration ID # 160152

**A. SCOPE OF SERVICES:**

A.1. The Contractor shall provide all service and deliverables as required, described, and detailed herein and shall meet all service and delivery timelines as specified by this Contract.

The Contractor shall provide configuration and implementation of the Microsoft Dynamics HHS Platform provided by the State which includes products listed in Attachment B. of this Contract.

The following documents, as may be amended by DIDD in the best interest of the State, shall be used as guidelines during the term of this contract:

- Attachment D. - Category Records
- Attachment E. - Project Charter

A.1.1. Project Approach

The State's Project Team resources will employ the Project Management Body of Knowledge (PMBOK) framework as a guide for working with the Contractor to successfully manage the project.

The State will commit the following full time equivalent resources for the duration of the project:

- BSD Senior Project Director.
- Business Requirements (*Attachment C - DIDD Business Requirements*) & Policy Leads and Subject Matter Experts from Planning, Financial, Protection from Harm and Quality Management areas.
- A Construction Team Lead/Liaison, DBA and System Architect interface between the Contractor and the State Office for Information Resources (OIR) for application and database construction and configuration activities.
- Infrastructure Lead to interface with the OIR regarding hardware, network and security activities.
- Conversion Team Lead.
- Testing Lead/Liaison.
- Implementation Lead.



- Training Lead/Liaison.
- The State requires that the Contractor's Team work side by side with the entire State Project Team, and to be fully cooperative and supportive of a close working relationship. The Contractor's Team will train, mentor, equip and enable the State Project Team to be full contributors throughout the project life cycle, to drive the project to successful completion, and to ultimately own, manage and support the System after implementation and other Contractor obligations are completed.

#### A.1.2. Contractor Requirements

1. The Project will include the following Milestone and deliverables.
  - a. Solution Design completion
    - i. Approval of all detail design documents for the total solution by the Project Steering Committee.
    - ii. Approval of the development and configuration schedule for each module for the solution by the Project Steering Committee.
    - iii. Approval of the detail testing plan for the entire development and implementation effort by the Project Steering Committee.
  - b. At the end of each of the three (3) module's implementation (Service Planning, Service Tracking & Billing, Quality & Protection from Harm).
    - i. Completion and DIDD acceptance of converted legacy systems data required for the module.
    - ii. User Acceptance Testing completed with no known high or medium severity defects for the phase currently being implemented or for previously implemented phases.
    - iii. Successful statewide implementation of the scheduled phase with signoff of the Project Steering Committee.
    - iv. User training for the module completed for all State users and Provider users.
    - v. User and Technical documentation for the module completed, accepted and distributed to appropriate users.
  - c. DIDD acceptance of ownership of the solution.
    - i. All deliverables completed, reviewed and approved.
    - ii. All performance criteria met or exceeded.
    - iii. DIDD sign-off of project completion.
  - d. End of Warranty Period.
2. The Contractor will design and assist in the statewide implementation of a solution that meets DIDD's business requirements as referenced in Attachment C. of this Contract. This design will include a Roles based security module that will allow the business to easily manage user access to the solution. This security system will be in compliance with the State's Enterprise Security Standards found in Attachment I. of this Contract.
3. The Contractor will insure that the response-time will average less than three seconds and never exceed five seconds, for all online activities conducted across the State



network. Response-time must be maintained at State WAN bandwidth utilization of up to 80%. Response-time is defined as the amount of time between pressing the "RETURN" or "ENTER" key or depressing a mouse button and receiving a data-driven response on the screen, not just a message or indicator that a response is forthcoming.

4. The Contractor will develop detail design documentation based on collaboration with the department's project team members, DIDD users and the high level requirements identified in Attachment C. of this Contract.
5. The Contractor will provide experienced Microsoft SQL database leadership for the design, configuration, implementation and support of the solution. The State approval is required for any changes to the project scope or schedule as well as Contractor personnel changes.
6. The Contractor will provide experienced Microsoft Dynamics HHS framework developers to design, develop, test and support the solutions. The State approval is required for any changes to the project scope or schedule as well as Contractor personnel changes
7. The Contractor shall provide a one-year (twelve-month, 365 day) Warranty Period for the Contractor-provided software. The Warranty Period begins upon acceptance of total ownership of the Contractor-provided software by technical and business management. During the one-year Warranty Period, the Contractor:
  - a. Shall perform warranty services at no cost to the State;
  - b. Shall be the initial contact point for all warranty notifications and support requests, regardless of the perceived source of the problem;
  - c. Shall correct any function, feature, or performance deficiency of the Contractor-provided software which does not conform to the Contract requirements and approved specifications (including implemented change requests); and
  - d. Shall respond to a report of an error the State deems "critical" within two hours. (A critical error is defined as one that would cause damage to the State system(s) or associated data, or would otherwise seriously impair the ability of users of the system(s) to do their jobs or the functions for which the system was established.)

The State will be the sole judge of the acceptability of warranty work.

8. The Contractor will participate in the development, testing and execution of the Conversion plans for each module. While DIDD will lead the technical effort of scrubbing and extracting legacy system data, the Contractor will assist in the data mapping process and be responsible for the integration of the converted data into the solution's database.
9. The Contractor will be an integral member of the Project Team.
10. The Contractor will participate in the management of the project within the adopted project management methodology and under the direction of the Project Director, Project Steering Committee, and Project Sponsor. The Contractor will actively participate in the integrated management of the project.
11. The Contractor will provide weekly project status updates, to include, but not limited to, reporting of actual hours expended, work accomplished, resource balancing issues, technical issues, resource risks and technical risks.



12. The Contractor will develop a plan for the detailed design phase of the project. The plan will include the activities, resources and approach to successfully collaborate with the State's business and technical stakeholders in identifying State's expectations, analyzing the requirements, mapping the processes, recognizing any gaps and creating an amenable solution design.
13. The Contractor will provide a detailed testing plan for the project to include, but not limited to, the State's responsibilities, testing assumptions, test case development, testing processes, testing tools, defect management processes and reporting, conversion tests, regression testing and stress testing.
14. The Contractor will review the initial hardware and network configuration plan and provide suggested improvements and the associated justifications. (See Attachment F. of this Contract)
15. The Contractor will create a realistic schedule for the development and implementation of the solution identifying the responsibilities of both the Contractor's and DIDD's resources in collaboration with the project team. This schedule will be submitted for review, approval, and integration into the overall project schedule.
16. The Contractor is responsible for the development and execution of a detailed training plan for the DIDD users, providers, and the technical support staff to include the development of criteria, materials, course content and student, instructor and course evaluations. The Contractor's training requirements for this project are to train approximately twenty-five (25) DIDD trainers who will then train twenty-three (2300) internal business users and twenty-five hundred (2500) external business users across three regions of the State of Tennessee. The Contractor will also be responsible to training thirty (30) technical staff to support the system. The Contractor will also be responsible for updating training materials based on the feedback and results of the initial train-the-trainer class and for maintaining the training materials to be current with any system configuration or modifications during the training rollout. DIDD will arrange the required facilities based on the Training Plan.
17. The Contractor will provide a detailed report identifying planned effort allocated by resource by module. All project related activities will be performed on site in association with DIDD business and technical resources unless agreed by to as an exception by the Project Director and the Project Steering Committee.
18. The Contractor will not make any changes to the design, configuration, code or schedule without the approval of the Change Control Board using the Change Control processes and procedures as defined in Section A.1.3. of this Contract and Attachment G. of this Contract.
19. The Contractor will participate as an advisor to the Change Control Board in the change control process by providing suggestions, alternatives, costs and schedule impact assessments for change request.
20. The Contractor shall complete all approved change orders. The State will be the sole judge of the acceptable completion of the change order work, and upon such determination, shall provide the Contractor with written approval.
21. The State will remunerate the Contractor for any approved change order only after acceptance of the change by the State and the implementation of said change order into production. If the change order is completed prior to implementation of the module or modules affected, the remuneration will be made after the affected module is successfully implemented. In the case where a Change Order affects more than one module, Remuneration will occur when the last affected module is implemented.



### A.1.3. Change Orders

The State may, at its sole discretion and with written notice to the Contractor, request changes in the scope of services that are necessary but were inadvertently unspecified in the scope of services of this Contract.

- a. Memorandum of Understanding (MOU) — after receipt of a written request for additional services from the State, the Contractor shall respond to the State, within a maximum of ten (10) business days, with a written proposal for completing the service. Said proposal must specify:
  - (1) the effect, if any, of implementing the requested change(s) on all other services required under this Contract;
  - (2) the specific effort involved in completing the change(s);
  - (3) the expected schedule for completing the change(s);
  - (4) the maximum number of person hours required for the change(s); and
  - (5) the maximum cost for the change(s) — this maximum cost shall in no instance exceed the product of the person hours required multiplied by the appropriate payment rate proposed for such work.

The Contractor shall not perform any additional service until the State has approved the proposal. If approved, the State will sign the proposal, and it shall constitute a MOU between the Contract Parties pertaining to the specified change(s) and shall be incorporated, hereby, as a part of this Contract.

- b. MOU Performance — Subsequent to State approval of a MOU, the Contractor shall complete the required services. The State will be the sole judge of the acceptable completion of work and, upon such determination, shall provide the Contractor written approval.
- c. MOU Remuneration — The State will remunerate the Contractor only for acceptable work. All acceptable work performed pursuant to an approved MOU, without a formal amendment of this Contract, shall be remunerated in accordance with and further limited by Section C.3.c. of this Contract, PROVIDED THAT, the State shall be liable to the Contractor only for the cost of the actual person hours worked to complete the necessary work, not to exceed the maximum cost for the change detailed in the MOU. In no instance shall the State be liable to the Contractor for the cost of any person hours worked in excess of the maximum person hours indicated in or of any amount exceeding the maximum cost specified by the approved MOU authorizing the service. Upon State approval of the work, the Contractor shall invoice the State in accordance with the relevant provisions of this Contract.

### **B. CONTRACT PERIOD:**

This Contract shall be effective for the period beginning November 17, 2012, and ending on or no later than November 16, 2014. The Contractor hereby acknowledges and affirms that the State shall have no obligation for services rendered by the Contractor which were not performed within this specified contract period.

### **C. PAYMENT TERMS AND CONDITIONS:**

- C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed one million, two hundred eighty six thousand, five hundred sixty dollars and no cents (\$1,286,560.00). The payment rates in section C.3 shall constitute the entire compensation due the Contractor for all service and Contractor obligations hereunder regardless of the difficulty, materials or equipment required. The payment rates include, but are not limited to, all applicable



taxes, fees, overheads, and all other direct and indirect costs incurred or to be incurred by the Contractor.

The Contractor is not entitled to be paid the maximum liability for any period under the Contract or any extensions of the Contract for work not requested by the State. The maximum liability represents available funds for payment to the Contractor and does not guarantee payment of any such funds to the Contractor under this Contract unless the State requests work and the Contractor performs said work. In which case, the Contractor shall be paid in accordance with the payment rates detailed in section C.3. The State is under no obligation to request work from the Contractor in any specific dollar amounts or to request any work at all from the Contractor during any period of this Contract.

- C.2. Compensation Firm. The payment rates and the maximum liability of the State under this Contract are firm for the duration of the Contract and are not subject to escalation for any reason unless amended.
- C.3. Payment Methodology. The Contractor shall be compensated based on the payment rates herein for units of service authorized by the State in a total amount not to exceed the Contract Maximum Liability established in section C.1.
  - a. The Contractor’s compensation shall be contingent upon the satisfactory completion of units, milestones, or increments of service defined in section A.
  - b. The Contractor shall be compensated for said units, milestones, or increments of service based upon the following payment rates:

<b>Service Description</b>	<b>Amount</b> (per compensable increment)
Acceptance by DIDD of the delivery of complete design documentation for all phases of the project.	\$ 233,920.00 20% of the Total Evaluation Cost Amount
Acceptance by DIDD of the delivery and implementation of the Service Planning phase of the project.	\$ 233,920.00 20% of the Total Evaluation Cost Amount
Acceptance by DIDD of the delivery and implementation of the Service Tracking & Billing phase of the project.	\$ 175,440.00 15% of the Total Evaluation Cost Amount
Acceptance by DIDD of the delivery and implementation of the Quality & Protection from Harm phase of the project.	\$ 175,440.00 15% of the Total Evaluation Cost Amount
Acceptance of total ownership of application by DIDD technical and business management.	\$ 233,920.00 20% of the Total Evaluation Cost Amount
End of Warranty Period	\$ 116,960.00 10% of the Total Evaluation Cost Amount



- c. The Contractor shall be compensated for changes requested and performed pursuant to Contract Section A.1.3., without a formal amendment of this contract based upon the payment rates detailed in the schedule below and as agreed pursuant to said Section A.1.3., PROVIDED THAT compensation to the Contractor for such “change order” work shall not exceed ten percent (10 %) of the sum of milestone payment rates detailed in Section C.3.b., above (which is the total cost for the milestones and associated deliverables set forth in Contract Sections A.1.2.3., through A.1.2.7.). If, at any point during the Contract period, the State determines that the cost of necessary “change order” work would exceed said maximum amount, the State may amend this Contract to address the need.

<b>Service Description</b> <b>CHANGE ORDER WORK</b>	<b>Amount</b> (per compensable increment)
PM (MCG)	\$ 225.00 per hour
BA1	\$ 195.00 per hour
BA2	\$ 195.00 per hour
Architect	\$ 250.00 per hour
Dev 1	\$ 185.00 per hour
Dev 2	\$ 185.00 per hour
Train Lead (Tanner)	\$ 180.00 per hour
Tran2 (Tanner)	\$ 155.00 per hour
UI Dev	\$ 115.00 per hour
<b>NOTE:</b> The Contractor shall not be compensated for travel time to the primary location of service provision.	

- C.4 Retention of Final Payment. The State shall withhold one hundred sixteen thousand, nine hundred sixty dollars and no cents (\$116,960.00), representing ten percent (10%) of the service increment amounts in table C.3.b. until the completion of the Warranty Period specified in Contract Section A.1.2.7.
- C.5 Travel Compensation. The Contractor shall not be compensated or reimbursed for travel, meals, or lodging.
- C.6 Invoice Requirements. The Contractor shall invoice the State only for completed increments of service and for the amount stipulated in section C.3, above, and present said invoices no more often than monthly, with all necessary supporting documentation, to:

Russell Nicoll, Chief Information Officer  
 Department of Intellectual and Developmental Disabilities  
 Andrew Jackson Building, 15<sup>th</sup> Floor  
 500 Deaderick Street  
 Nashville, Tennessee 37243

- a. Each invoice shall clearly and accurately detail all of the following required information (calculations must be extended and totaled correctly).
  - (1) Invoice Number (assigned by the Contractor)



- (2) Invoice Date
- (3) Contract Number (assigned by the State)
- (4) Customer Account Name: Department of Intellectual and Developmental Disabilities
- (5) Customer Account Number (assigned by the Contractor to the above-referenced Customer)
- (6) Contractor Name
- (7) Contractor Tennessee Edison Registration ID Number Referenced in Preamble of this Contract
- (8) Contractor Contact for Invoice Questions (name, phone, and/or fax)
- (9) Contractor Remittance Address
- (10) Description of Delivered Service
- (11) Complete Itemization of Charges, which shall detail the following:

- i. Service or Milestone Description (including name & title as applicable) of each service invoiced
- ii. Number of Completed Units, Increments, Hours, or Days as applicable, of each service invoiced
- iii. Applicable Payment Rate (as stipulated in Section C.3.) of each service invoiced
- iv. Amount Due by Service
- v. Total Amount Due for the invoice period

b. The Contractor understands and agrees that an invoice under this Contract shall:

- (1) include only charges for service described in Contract Section A and in accordance with payment terms and conditions set forth in Contract Section C;
- (2) only be submitted for completed service and shall not include any charge for future work;
- (3) not include sales tax or shipping charges; and
- (4) initiate the timeframe for payment (and any discounts) only when the State is in receipt of the invoice, and the invoice meets the minimum requirements of this section C.6.

C.7. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or matter in relation thereto. A payment by the State shall not be construed as acceptance of any part of the work or service provided or as approval of any amount invoiced.

C.8. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment theretofore made which are determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, not to constitute proper remuneration for compensable services.

C.9. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee any amounts, which are or shall become due and payable to the State of Tennessee by the Contractor.

C.10. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following documentation properly completed.

- a. The Contractor shall complete, sign, and present to the State an "Authorization Agreement for Automatic Deposit (ACH Credits) Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once said form is received by the State, all payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee shall be made by Automated Clearing House (ACH).



- b. The Contractor shall complete, sign, and present to the State a "Substitute W-9 Form" provided by the State. The taxpayer identification number detailed by said form must agree with the Contractor's Federal Employer Identification Number or Tennessee Edison Registration ID referenced in this Contract.

**D. STANDARD TERMS AND CONDITIONS:**

- D.1. Required Approvals. The State is not bound by this Contract until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).
- D.2. Modification and Amendment. This Contract may be modified only by a written amendment signed by all parties hereto and approved by both the officials who approved the base contract and, depending upon the specifics of the contract as amended, any additional officials required by Tennessee laws and regulations (said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).
- D.3. Termination for Convenience. The State may terminate this Contract without cause for any reason. Said termination shall not be deemed a breach of contract by the State. The State shall give the Contractor at least thirty (30) days written notice before the effective termination date. The Contractor shall be entitled to compensation for satisfactory, authorized service completed as of the termination date, but in no event shall the State be liable to the Contractor for compensation for any service which has not been rendered. Upon such termination, the Contractor shall have no right to any actual general, special, incidental, consequential, or any other damages whatsoever of any description or amount.
- D.4. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor violates any terms of this Contract, the State shall have the right to immediately terminate the Contract and withhold payments in excess of fair compensation for completed services. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any breach of this Contract by the Contractor.
- D.5. Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the services performed under this Contract without obtaining the prior written approval of the State. If such subcontracts are approved by the State, each shall contain, at a minimum, sections of this Contract below pertaining to "Conflicts of Interest," "Nondiscrimination," and "Records" (as identified by the section headings). Notwithstanding any use of approved subcontractors, the Contractor shall be the prime contractor and shall be responsible for all work performed.
- D.6. Conflicts of Interest. The Contractor warrants that no part of the total Contract Amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed relative to this Contract.
- The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six months has been, an employee of the State of Tennessee.
- D.7. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, color, religion, sex, national origin, or any other classification protected by Federal, Tennessee State constitutional, or statutory law. The



Contractor shall, upon request, show proof of such nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

- D.8. Prohibition of Illegal Immigrants. The requirements of *Tennessee Code Annotated*, Section 12-4-124, *et seq.*, addressing the use of illegal immigrants in the performance of any Contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.
- a. The Contractor hereby attests, certifies, warrants, and assures that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment A., hereto, semi-annually during the period of this Contract. Such attestations shall be maintained by the Contractor and made available to state officials upon request.
  - b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the period of this Contract, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work relative to this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work relative to this Contract. Attestations obtained from such subcontractors shall be maintained by the Contractor and made available to state officials upon request.
  - c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Said records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.
  - d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of *Tennessee Code Annotated*, Section 12-4-124, *et seq.* for acts or omissions occurring after its effective date. This law requires the Commissioner of Finance and Administration to prohibit a contractor from contracting with, or submitting an offer, proposal, or bid to contract with the State of Tennessee to supply goods or services for a period of one year after a contractor is discovered to have knowingly used the services of illegal immigrants during the performance of this Contract.
  - e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not either a United States citizen, a Lawful Permanent Resident, or a person whose physical presence in the United States is authorized or allowed by the federal Department of Homeland Security and who, under federal immigration laws and/or regulations, is authorized to be employed in the U.S. or is otherwise authorized to provide services under the Contract.
- D.9. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, insofar as they relate to work performed or money received under this Contract, shall be maintained for a period of three (3) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.
- D.10. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.



- D.11. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.
- D.12. Strict Performance. Failure by any party to this Contract to insist in any one or more cases upon the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any such term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the parties hereto.
- D.13. Independent Contractor. The parties hereto, in the performance of this Contract, shall not act as employees, partners, joint venturers, or associates of one another. It is expressly acknowledged by the parties hereto that such parties are independent contracting entities and that nothing in this Contract shall be construed to create an employer/employee relationship or to allow either to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever.
- The Contractor, being an independent contractor and not an employee of the State, agrees to carry adequate public liability and other appropriate forms of insurance, including adequate public liability and other appropriate forms of insurance on the Contractor's employees, and to pay all applicable taxes incident to this Contract.
- D.14. State Liability. The State shall have no liability except as specifically provided in this Contract.
- D.15. Force Majeure. The obligations of the parties to this Contract are subject to prevention by causes beyond the parties' control that could not be avoided by the exercise of due care including, but not limited to, natural disasters, riots, wars, epidemics, or any other similar cause.
- D.16. State and Federal Compliance. The Contractor shall comply with all applicable State and Federal laws and regulations in the performance of this Contract.
- D.17. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Contractor agrees that it will be subject to the exclusive jurisdiction of the courts of the State of Tennessee in actions that may arise under this Contract. The Contractor acknowledges and agrees that any rights or claims against the State of Tennessee or its employees hereunder, and any remedies arising therefrom, shall be subject to and limited to those rights and remedies, if any, available under *Tennessee Code Annotated*, Sections 9-8-101 through 9-8-407.
- D.18. Completeness. This Contract is complete and contains the entire understanding between the parties relating to the subject matter contained herein, including all the terms and conditions of the parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the parties relating hereto, whether written or oral.
- D.19. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions hereof shall not be affected thereby and shall remain in full force and effect. To this end, the terms and conditions of this Contract are declared severable.
- D.20. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

**E. SPECIAL TERMS AND CONDITIONS:**

- E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, these special terms and conditions shall control.



- E.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by EMAIL or facsimile transmission with recipient confirmation. Any such communications, regardless of method of transmission, shall be addressed to the respective party at the appropriate mailing address, facsimile number, or EMAIL address as set forth below or to that of such other party or address, as may be hereafter specified by written notice.

The State:

Russell Nicoll, Chief Information Officer  
Department of Intellectual and Developmental Disabilities  
Andrew Jackson Building, 15<sup>th</sup> Floor  
500 Deaderick Street  
Nashville, Tennessee 37243  
Russell.Nicoll@tn.gov  
Telephone (615) 975-3897  
FAX # (615) 391-9841

The Contractor:

John L. Malcolm, Vice President of the Dynamics Practice  
Mid-America Consulting Group, Inc.  
3700 Euclid Ave, Second Floor  
Cleveland, Ohio 44115  
John.Malcolm@mcgcorp.com  
Telephone # (216) 374-6906  
FAX # (216) 432-6925

All instructions, notices, consents, demands, or other communications shall be considered effectively given upon receipt or recipient confirmation as may be required.

- E.3. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State and/or Federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate the Contract upon written notice to the Contractor. Said termination shall not be deemed a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. Should such an event occur, the Contractor shall be entitled to compensation for all satisfactory and authorized services completed as of the termination date. Upon such termination, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages whatsoever of any description or amount.
- E.4. Tennessee Consolidated Retirement System. The Contractor acknowledges and understands that, subject to statutory exceptions contained in *Tennessee Code Annotated*, Section 8-36-801, *et. seq.*, the law governing the Tennessee Consolidated Retirement System (TCRS), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established pursuant to *Tennessee Code Annotated*, Title 8, Chapter 35, Part 3 accepts state employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the period of this Contract.
- E.5. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State



or acquired by the Contractor on behalf of the State shall be regarded as confidential information in accordance with the provisions of applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards. Such confidential information shall not be disclosed, and all necessary steps shall be taken by the Contractor to safeguard the confidentiality of such material or information in conformance with applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards.

The Contractor's obligations under this section do not apply to information in the public domain; entering the public domain but not from a breach by the Contractor of this Contract; previously possessed by the Contractor without written obligations to the State to protect it; acquired by the Contractor without written restrictions against disclosure from a third party which, to the Contractor's knowledge, is free to disclose the information; independently developed by the Contractor without the use of the State's information; or, disclosed by the State to others without restrictions against disclosure. Nothing in this paragraph shall permit Contractor to disclose any information that is confidential under federal or state law or regulations, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties.

It is expressly understood and agreed the obligations set forth in this section shall survive the termination of this Contract.

- E.6. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.
- a. Contractor warrants to the State that it is familiar with the requirements of HIPAA and its accompanying regulations, and will comply with all applicable HIPAA requirements in the course of this Contract.
  - b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by HIPAA and its regulations, in the course of performance of the Contract so that both parties will be in compliance with HIPAA.
  - c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by HIPAA and that are reasonably necessary to keep the State and Contractor in compliance with HIPAA. This provision shall not apply if information received by the State under this Contract is NOT "protected health information" as defined by HIPAA, or if HIPAA permits the State to receive such information without entering into a business associate agreement or signing another such document.
- E.7. State Ownership of Work Products. The State shall have ownership, right, title, and interest, including ownership of copyright, in all work products, including computer source code, created, designed, developed, derived, documented, installed, or delivered under this Contract subject to the next subsection and full and final payment for each "Work Product." The State shall have royalty-free and unlimited rights and license to use, disclose, reproduce, publish, distribute, modify, maintain, or create derivative works from, for any purpose whatsoever, all said Work Products.
- a. To the extent that the Contractor uses any of its pre-existing, proprietary or independently developed tools, materials or information ("Contractor Materials"), the Contractor shall retain all right, title and interest in and to such Contractor Materials, and the State shall acquire no right, title or interest in or to such Contractor Materials EXCEPT the Contractor grants to the State an unlimited, non-transferable license to use, copy and distribute internally, solely for the State's internal purposes, any Contractor Materials reasonably associated with any Work Product provided under the Contract.
  - b. The Contractor shall furnish such information and data as the State may request, including but not limited to computer code, that is applicable, essential, fundamental, or



intrinsic to any Work Product and Contractor Materials reasonably associated with any Work Product, in accordance with this Contract and applicable state law.

- c. Nothing in this Contract shall prohibit the Contractor's use for its own purposes of the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of providing the services requested under this Contract.
- d. Nothing in the Contract shall prohibit the Contractor from developing for itself, or for others, materials which are similar to and/or competitive with those that are produced under this Contract.

E.8. Ownership of Software and Work Products.

a. Definitions.

- (1) "Contractor-Owned Software," which shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.
- (2) "Custom-Developed Application Software," which shall mean customized application software developed by Contractor solely for State.
- (3) "Rights Transfer Application Software," which shall mean any pre-existing application software owned by Contractor or a third party, provided to State and to which Contractor will grant and assign, or will facilitate the granting and assignment of, all rights, including the source code, to State.
- (4) "Third-Party Software," which shall mean software not owned by the State or the Contractor.
- (5) "Work Product," which shall mean all deliverables exclusive of hardware, such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor for the State during the course of the project using State's money or resources, including Custom-Developed Application Software. If the system solution includes Rights Transfer Application Software, the definition of Work Product shall also include such software.

b. Rights and Title to the Software

- (1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license granted herein.
- (2) All right, title and interest in and to the Work Product, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other intellectual property and other proprietary rights embodied by and arising out of the Work Product, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Work Product, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Work Product. Contractor shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer and/or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties, and Contractor shall cooperate fully in the foregoing endeavors.
- (3) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted thereby.



- c. Nothing in this Contract shall prohibit the Contractor's use for its own purposes of the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of providing the services requested under this Contract.
  - d. Nothing in this Contract shall prohibit the Contractor from developing for itself, or for others, materials which are similar to and/or competitive with those that are produced under this Contract.
- E.9. State Furnished Property. The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible, personal property furnished by the State for the Contractor's temporary use under this Contract. Upon termination of this Contract, all property furnished shall be returned to the State in good order and condition as when received, reasonable use and wear thereof excepted. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the residual value of the property at the time of loss.
- E.10. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below.
- a. this Contract document with any attachments or exhibits (excluding the items listed at subsections b. through e., below);
  - b. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
  - c. the State solicitation, as may be amended, requesting proposals in competition for this Contract;
  - d. any technical specifications provided to proposers during the procurement process to award this Contract;
  - e. the Contractor's proposal seeking this Contract.
- E.11. Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:
- a. No federally appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
  - b. If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.
  - c. The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.



This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, *U.S. Code*.

E.12. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
- b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
- c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and
- d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

E.13. Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's proposal responding to RFP-34401-00420 (Attachment 6.2. – Section B.) and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and persons with a disability. Such reports shall be provided to the state of Tennessee Governor's Office of Diversity Business Enterprise in form and substance as required by said office.

E.14. Standard Software In the event that the Contractor wishes to introduce non-State standard software or hardware components ("products") into the State's technology environment, in support of, or related to, the services the Contractor is providing under this Contract, the Contractor must make a formal written request to the State prior to introducing the non-State Standard Products. Such a request is referred to as a "Non-State Standard Product Request."

- a. Non-State Standard Products are defined as:
  - Any software that is not listed and designated as Current in the *State of Tennessee Enterprise Architecture (Attachment H)*, as amended; or
  - Any hardware that is not listed and designated as Current in, or is not compatible with standards listed in, the *Tennessee Enterprise Architecture*, as amended.
- b. The State's Department of Finance and Administration, Office for Information Resources (OIR), shall consider the Non-State Standard Product Request and shall render a written determination, in the State's best interest, to approve or disapprove the request. If OIR disapproves the request, the Contractor agrees to withdraw the request and substitute State Standard Products in place of the Non-State Standard Products, at no additional cost to the State.



IN WITNESS WHEREOF,

MID-AMERICA CONSULTING GROUP, INC.:



12/14/12

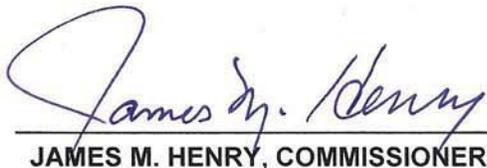
CONTRACTOR SIGNATURE

DATE

JOHN L. MALCOLM, VICE PRESIDENT OF THE DYNAMICS PRACTICE

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF INTELLECTUAL AND DEVELOPMENTAL DISABILITIES:



12-4-12

JAMES M. HENRY, COMMISSIONER

DATE



**ATTACHMENT A**

**ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE**

<b>SUBJECT CONTRACT NUMBER:</b>	35033
<b>CONTRACTOR LEGAL ENTITY NAME:</b>	<b>MID-AMERICA CONSULTING GROUP, INC.:</b>
<b>FEDERAL EMPLOYER IDENTIFICATION NUMBER: (or Social Security Number)</b>	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

**CONTRACTOR SIGNATURE**

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. If said individual is not the chief executive or president, this document shall attach evidence showing the individual's authority to contractually bind the Contractor.

**JOHN L. MALCOLM, VICE PRESIDENT OF THE DYNAMICS PRACTICE**

**PRINTED NAME AND TITLE OF SIGNATORY**

12/14/12

**DATE OF ATTESTATION**



## Microsoft Dynamics Product Listing

Product Description	Mfg #	Quantity
DYNCRMCAL ALNG LICSA PK MVL DVCCAL	ZFA-00245	28000
DYNCRMCAL ALNG LICSA PK MVL USRCAL	ZFA-00237	2400
DYNCRMSVR ALNG LICSA PK MVL	N9J-00523	2
DYNCRMEXTCONN ALNG LICSA PK MVL	ZGA-00122	2
DYNGPAMCAL ALNG LICSA PK MVL US USRCAL	CRA-00012	10
DYNGPAMSVR ALNG LICSA PK MVL US	CAN-00008	1
DYNGPBSCCAL ALNG LICSA PK MVL US USRCAL	M9D-00008	100
DYNGPDEVTOOLS ALNG LICSA PK MVL US	LUW-00005	1
SHAREPOINTINTRNTSITESENT ALNG LICSA PK MVL	CKF-00298	2



## DIDD Business Requirements

#	Category	Business Requirements
1	Persons	The system will capture, track, and maintain information for all persons served by DIDD from the point of initial contact through the life cycle of the client record.
2	Persons	Upon entry of a new client record, the system will perform a search for potential duplicate client records, and the system will provide the user with a warning that a potential duplicate record exists.
3	Persons	The system must be capable of merging any duplicate record created in error.
4	Persons	The system must be capable of using web services to validate client demographic information such as SSN, Address, etc.
5	Persons	The system will allow for additional client records fields to become available for data entry based on the Person's status in the system and on where the Person is in the enrollment process, such as initial contact, wait list, enrollment, etc.
6	Persons	System will provide auditable history of all changes made to a person's information, including the value(s) changed, who made the change, the time and date of the change and the reason or authorization for the change.
7	Persons	The system will provide alerts and/or notifications to users (via workflow rules) for additions and changes to personal information.
8	Persons	The system will be designed in order to support a workflow for Case Management for Persons beginning at the point of initial contact, and must support assignment and reassignment of Persons throughout the life cycle of the client record.
9	Persons	The system will allow the entry of comments and notes related to the person by authorized users. These comments and notes should be viewable by authorized users as part of the client record.
10	Persons	The system will provide the ability to attach scanned or system generated documents, including emails, to a client record. Attachments to a client record will be viewable by authorized users.
11	Persons	Upon service enrollment, the system will be configured to prevent Persons from being enrolled in multiple waivers during the same time period.
12	Persons	The system will allow for both pre-defined and ad hoc user-defined reporting capabilities, and should provide users with the option of viewing the information in summary or detailed formats.
13	Planning	The system will provide the ability to create and modify an Individual Service Plan (ISP) for a person of PAE or enrollment status.
14	Planning	The system will provide data entry edits for the creation and maintenance of the ISP. The user will receive real time messages for errors and inconsistencies for their immediate correction.
15	Planning	The system will provide the ability for Waiver information to be maintained in the system.
16	Planning	The system will verify the services, date range for the service and any cost restrictions entered into the ISP are in compliance with the waiver in which the person is enrolled. The system will issue warnings for services selected outside of the waiver or other inconsistencies. User can override the warnings and submit for approval.
17	Planning	The system will provide a workflow for the plan approval process.



		The rules of the workflow will be managed by the DIDD Staff.
18	Planning	The system will allow ISP amendments to be processed in a similar fashion as the original ISP's.
19	Planning	The system will provide alerts and notifications to the appropriate people for plan and service approvals and denials.
20	Providers	The system will provide a lookup function during plan development that will display all current providers of the requested service, based on the geographic area of the person being served.
21	Providers	The system will support a workflow process for the creation and review of an ISP
22	Providers	The system will support a workflow for the ISP appeal and disposition processes.
23	Providers	The system will capture, track, and maintain information for all DIDD service providers from the point of initial contact through the life cycle of the provider record, including information related to the provider approval process. The system will track all relevant provider information, including but not limited to licensure data, authorized services, and locations.
24	Providers	The system will allow the data entry and management of services authorized for a provider at a specific location.
25	Providers	System will provide auditable history of all changes made to a provider's information, including the value(s) changed, who made the change, the time and date of the change and the reason and/or authorization for the change.
26	Providers	The system will track comments and notes of an authorized user regarding the provider. The comments will be accessible based on the user's role.
27	Providers	The system will provide the ability for scanned documents to be linked to the provider and viewable by authorized users.
28	Services	The system will provide the ability to setup and maintain any and all services and associate them to specific waivers and/or identified as a State service. Dates and codes will be used to activate and deactivate the services.
29	Services	System will provide auditable history of all changes made to the service's information, including the values being changed, who made the change, the time and date of the change and the reason and/or authorization for the change.
30	Services	The system will track comments and notes regarding the service made by anyone with the security. The comments will be accessible based on the user's role.
31	Services	The system will provide a method of linking services to each provider. Information unique to the provider and the service, i.e. cost of service, will be maintained in that link.
32	PFH	The system must provide users with the ability to enter incidents into the system.
33	PFH	The system must provide fundamental edits to insure the correctness of the data. Drop downs must provide options for user selection.
34	PFH	The system must allow for incidents to be linked to persons, providers, other entities interventions and other incidents.
35	PFH	Within an incident there must be the ability to choose multiple incident types.
36	PFH	There must be the ability to select multiple interventions for an incident.



37	PFH	The system must provide the ability for the creation, deletion and updating of workflow processing rules and timings for the processing of incidents and investigations.
38	PFH	The System must allow the assignment and reassignment of investigators to an investigation.
39	PFH	The system must track notes regarding an investigation by an authorized person. The comments must be accessible based on the user's role.
40	PFH	The system must generate alerts and notices regarding incidents and investigations per the workflow rules.
41	PFH	The system must produce standard incident and Investigation reports that are security and user parameter driven.
42	PFH	The system must be able to generate an investigation closed report from the data collected and stored in the database.
43	Claims	The system must provide a GUI to allow the provider to enter a claim for service in real time. The GUI must validate the claim against the Person being served information, the eligible provider services, the Individual Service Plan (ISP), the services dates and the service rules to insure accuracy.
44	Claims	The system must recognize the funding source for a specific service for a specific data and route the financial transaction appropriately.
45	Claims	The system must provide an override capability for items on a claim following workflow rules.
46	Claims	The system must provide the ability for comments regarding the claim to be entered into a log and the ability for authorized users to view those comments.
47	Claims	The system must provide a batched claims process that allows the provider to submit claims via an upload. The system must generate an acknowledgement for the data received to the provider.
48	Claims	The system must process the batched claims for a provider using the same edit logic that is used for the GUI entered claims. Erred claims will be placed in suspension and the provider notified of the claim and its errors.
49	Claims	The system will allow providers to use the GUI to view and edit their claims that are in a suspended mode. It will use the same edit logic as claim entry.
50	Claims	The system must format the appropriate claims to the EDI 837 transaction format.
51	Claims	The system must process the EDI 835 acknowledgements against the claims sent to update the claim status
52	Claims	The system must provide the provider with the ability to inquire on any of their claims and see details regarding the status, location in the workflow, denials, etc.
53	Claims	The system must provide total access to claims information for secured DIDD staff.
54	Claims	The system must provide history of claims and payments for a provider. Parameters as to time period, Service, Person being served, status, etc. will drive the content of the report.
55	Claims	The system must provide a claims reconciliation report and/or inquiry window for both providers and DIDD staff.
56	Claims	The system must provide specific DIDD staff the ability to update and override claims information to expedite or restrict processing and payment.



57	Security	The system will provide users with secure access to the application and data within the application based upon the user's profile (Roles and Responsibilities).
58	Security	The system will limit security controls to users based on their security profile
59	Security	The system will track all security changes for audit control.
60	Security	User's not included in the State's AD must have the ability to securely access the application.
61	General	The system must support the use of dashboards and reports to provide DIDD management with metrics and measurements as will be defined by management.
62	Performance	The system must be robust enough to allow 5000 users to be concurrently working in the application without degradation.



## Category Records

<b>Category</b>	<b>Annual Number of Records</b>	<b>Expected Annual Growth Rate</b>
Avg. Monthly Planning Transactions	6,781	Minimal
Avg. Monthly Incidents	1,056	Minimal
Avg. Monthly Investigations	158	Minimal
Total number of Persons being served (Referrals, Waitlist & Enrolled)	16,000	Minimal
Total Number of Providers	550	
Avg. Number of Claims processed per day	40,000	
Number of Internal Users	2300	Minimal
Number of External Users	2500	



**PROJECT CHARTER**  
**PROJECT TITAN**

**DEPARTMENT OF INTELLECTUAL AND DEVELOPMENTAL DISABILITIES**  
**15<sup>TH</sup> FLOOR, ANDREW JACKSON BUILDING**  
**500 DEADERICK STREET**  
**NASHVILLE, TN 37243**

**MAY 17, 2012**



**TABLE OF CONTENTS**

EXECUTIVE SUMMARY ..... 3

PROJECT PURPOSE/JUSTIFICATION ..... 3

Business Needs and Cases ..... 4

Business Objectives ..... 5

PROJECT DESCRIPTION ..... 8

Project Objectives and Success Criteria ..... 8

Requirements ..... 9

Constraints ..... 12

Assumptions ..... 13

Preliminary Scope Statement ..... 13

RISKS ..... 15

PROJECT DELIVERABLES ..... 16

SUMMARY MILESTONE SCHEDULE ..... 16

SUMMARY BUDGET ..... 16

ORGANIZATION AND RESPONSIBILITIES ..... 17

Project Team Staffing Estimate ..... 23

PROJECT APPROVAL REQUIREMENTS ..... 24

AUTHORIZATION ..... 24



## EXECUTIVE SUMMARY

Currently, the Department of Intellectual and Developmental Disabilities (DIDD) relies heavily on paper based, labor intensive and manual processes and some disparate computer applications to manage the support for persons served. This has resulted in a lack of standardized processes, silos of information and concerns regarding data integrity and reporting. Project Titan is focused on three programmatic areas: Planning, Protection from Harm and Financial Management. This effort will result in the standardization of processes using workflow rules, improvement in the timeliness and accuracy of data collection through online functionality and enhanced data visibility and reporting based on the application of a central data repository. These results are significant to DIDD's efforts to improve the effectiveness and efficiency of its staff and agencies in providing person centered services.

DIDD has engaged the Business Solutions Delivery (BSD) team to assist in the successful planning and execution of Project Titan. BSD provides a project management methodology based on best practices and the successes of its experienced team members.

## PROJECT PURPOSE/JUSTIFICATION

The Department of Intellectual and Developmental Disabilities is represented by over 2,800 employees, partnered with almost 500 provider agencies, provides services for over 8,000 individuals with intellectual disabilities and has approximately 7,200 individuals waiting to be enrolled in DIDD services. The current environment presents DIDD with challenges in realizing its mission. The overall objective of Project Titan is to address these challenges through the prudent use of technology, improved processes and procedures and better utilization of resources. A second objective is to provide a framework on which future innovative initiatives can be configured. Project Titan will focus on the three programmatic areas identified in the Executive Summary. These three areas encompass much of the core functionality of the Department's business. Across the three programmatic areas there are six apparent needs:

- Access to business information from a single repository
- Immediate access to current business information
- Continuous improvement of business processes
- User friendliness, portability and security to access and update information
- Flexibility to respond quickly and efficiently to changes to the business model and improvements in technology
- Improved utilization of human resources to support the Department's mission



## **Business Needs and Cases**

The Department needs to allow all authorized individuals to have the ability to access business information from a common repository. This will eliminate duplicate and inconsistent data, multiple silos of information and the interaction with multiple business systems and applications to complete a business task. In the Planning area, authorized users both within the State and provider communities will gain access to common and pertinent information about a person served while using the same application. In the Financial area, the Department will consolidate financial tracking and improve efficiencies. In the Protection from Harm area, authorized individuals will directly access all information relevant to incidents and investigations, reducing the risk of harm to individuals.

The Department needs immediate access to current business information. This will enable responsiveness to events, reduce the risk of errors and support better decision making. In the Planning area, the Department will track and dynamically respond to high frequency critical events that drive changes to Individual Support Plans. In the Financial area, the Department will complete real time service adjustments and claims processing, enhancing the financial stability of service providers. In the Protection from Harm area, the Department will access current safety information supporting reported incidents and investigations.

The Department needs to enhance its continuous process improvement with the use of technology. This will improve the Department's efficiency and effectiveness by enforcing standardized processes and metrics to evaluate business performance. In the Planning area, the Department will enforce standardized rule-based processes in order to establish benchmarks for evaluations and continuous improvement. In the Financial area, the Department will continuously incorporate best practices for leaner financial transactions and reporting to maximize federal reimbursements. In the Protection from Harm area, the Department will monitor and improve the performance of incident and investigation reporting and tracking tools in order to proactively address and enhance the safety of all persons.

The Department needs immediate user friendly, portable and secure access for the collection, review and reporting of agency information. This will allow DIDD employees, persons served and partners in all geographical locations secure access to appropriate and pertinent business information. In the Planning area, individuals will conveniently access and record information supporting individuals served. In the Financial area, authorized users will readily access, record, review and audit financial transactions and supporting information in a



secure environment. In the Protection from Harm area, individuals will remotely access, record and review information regarding incidents and investigations in a convenient, simple and secure way.

The Department needs flexibility to keep up with the external and internal factors that mandate business change. This will allow timely and thorough responsiveness to federal, judicial and State requirements as well as technological advancements that drive business change. In the Planning area, the Department will be able to tailor its enrollment processes to external and internal business drivers. In the Financial area, the Department will improve its interoperability between DIDD and its provider agencies and TennCare. In the Protection from Harm area, the Department will respond quickly to judicial mandates and have the ability to adopt new technologies as they become available in order to continuously monitor safety and decrease risks.

The Department needs to improve the effectiveness of its staff with a more efficient utilization of technology. By reducing the time consuming and error prone manual processes, department and provider staff can be refocused to more person centered responsibilities. In the Planning area, the enrollment, approval and oversight of services will gain efficiencies from the use of better technology. In the Financial area, the automation of financial transactions with our partners will remove many of the manual reconciliation efforts. In the Protection from Harm area, the real time capturing of information will reduce the incident and investigation data entry processes allowing for the allocation of human resources to other needs.

### **Business Objectives**

The mission of the Department of Intellectual and Developmental Disabilities is to use person centered practices to be a leader in the state service delivery system to support and increase the quality of life for Tennesseans with intellectual and developmental disabilities. To continuously support the Department's mission, multiple business reviews have been conducted. Through these reviews, a number of business objectives have been repeatedly identified. Project Titan will address these objectives, which consist of:

- Supporting the improvement of Protection from Harm by implementing a technology solution that reduces manual processes and improves data visibility, thus allowing staff to focus on their primary business goal of keeping people safe
- Improving both provider and Department financial integrity and flexibility to better facilitate tracking, validating and reporting of financial transactions through the use of an integrated technology solution



**ATTACHMENT E**

- Creating an electronic Individual Support Plan (ISP) which improves the ability to manage the services and outcomes that are provided to the persons served with a centralized repository and online information collection process

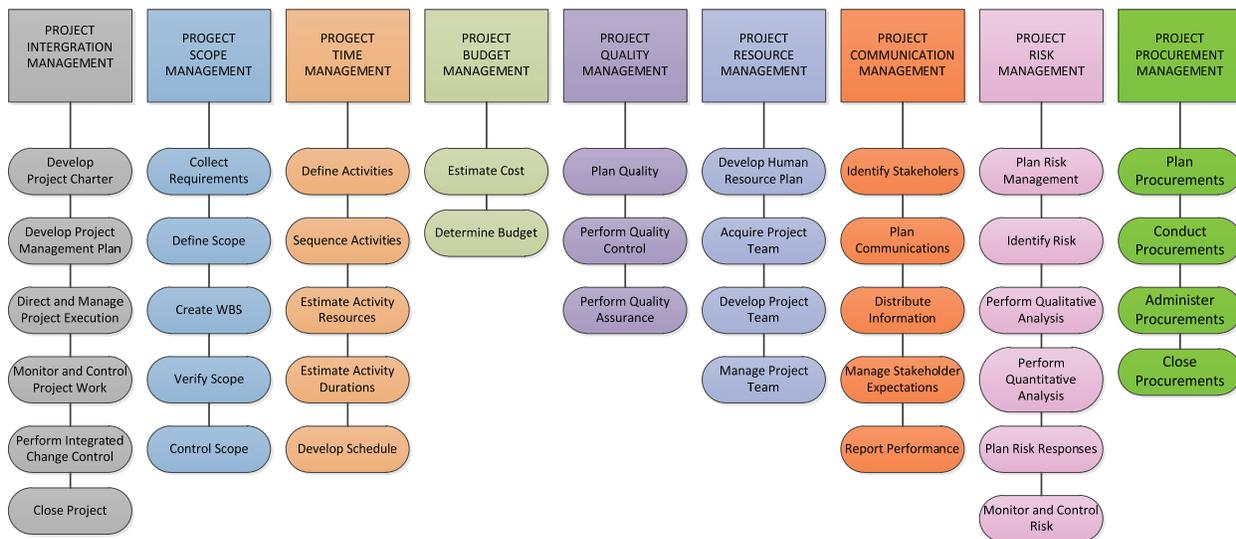


The success criteria for Project Titan will be to:

- Improve departmental decision making through access to current and accurate information
- Allow rule-based workflow technology for the collection, reporting and annotation of information related to providers, services and persons served
- Enable multilevel, role-based security allowing appropriate accessibility to information
- Improve financial audit support to allow standardization and better management of personal funds, trust accounts and third party liability within the Intermediate Care Facilities (ICF)
- Enhance the flexibility of business processes and systems to quickly adapt to future changes mandated by Federal, State and Legislative authorities
- Establish an electronic Individual Support Plan that is structured to be the cornerstone of future electronic records
- Provide current and accurate information to the courts
- Supply appropriate users with provider information related to demographics, services authorized and provider organization
- Provide adequate and accurate information about each person served

## PROJECT DESCRIPTION

Project Titan will be managed by closely ascribing to project management methodologies that are based on the Project Management Book of Knowledge (PMBOK) and have been adopted by the Business Solutions Delivery Team. The result of this approach will be the delivery of a quality product that meets the stakeholders’ defined requirements within the planned schedule and budget. The schematic below illustrates the methodology.



### Project Objectives and Success Criteria

The project management objectives for Project Titan are:

- Provide a quality solution that meets the project stakeholders’ expectations and defined requirements. This will be monitored and reported using the Requirements Traceability Matrix (RTM) and the recorded results of the User Acceptance Testing (UAT).
- Complete the project within the planned schedule. This will be monitored and reported using the Microsoft Project, Earned Value (EV) tools, Slipping and Slipped Tasks reports and other project monitoring reports and techniques. Changes to the schedule’s baseline will be managed through a formal Change Control Process.
- Complete the project within the planned budget. This will be monitored and reported by the tracking and periodic review of actual cost versus the budgeted expenses and the use of EV tools.
- Manage any and all changes to the original scope and requirements of the project. This will be monitored and managed via a Change Control



Board with established processes and guidelines to which strict adherence will be maintained.

- Ensure timely and appropriate generation, collection and distribution of all project information to the Project Steering Committee (PSC), Project Team and other project stakeholders. This will be monitored via meeting minutes, meeting notes and a communication registry that reflects the planned and actual formal communications to the PSC, Project Team and project stakeholders.
- Manage risks to the project by the use of a risk register. The risk register is used to identify all risks to the project, to quantify their probabilities of occurring, qualify their impact to the project and develop risk responses. The risk responses will be developed using expert judgment by the Project Director, Project Sponsor and Project Team.
- Manage the project procurement by following the State's procurement policies and procedures. Procurements will be monitored through a registry of purchasing documents (RFI, RFP, PO's, contracts, etc.) and through the budget review processes.
- Manage and monitor the acquisition, training and utilization of all project related human resources by use of organizational charts, conflict management techniques, status reports and meetings.

## Requirements

Below is the list of high-level project requirements that have been collected and reviewed by the Project Team and stakeholders. The high-level requirements are grouped into general categories.

- Online, real time user interface
  - Will provide access to authorized individuals which will support intake, service planning, provider management, incident and investigation reporting and tracking, claims processing and accounting
  - Will include data and system edits and controls to assure data quality
  - Will provide immediate visibility of collected data for authorized individuals
  - Will provide the ability to accommodate multiple user platforms
- Centralized data repository
  - Will provide a centralized system of record for all data related to persons served, providers, and services of DIDD
  - Will provide a sophisticated search engine to allow the identification of data elements related to persons served, providers and services
  - Will provide the ability to navigate across the data structure to analyze related data elements associated with persons served, providers and services



- Will support purging and archiving of data
- Distributed application
  - Will support a State standard system architecture that provides flexibility, adaptability and recoverability of data throughout the life-cycle of the application
  - Will support better management of the service level DIDD provides to its persons served, providers and other entities
- Document imaging and management
  - Will provide the ability to capture and securely store documents
  - Will allow authorized users to associate stored documents to persons served, provider and service records (i.e. incident forms, service plans, verification documents, diagnoses, EDI documents)
  - Will provide the controls to ensure the integrity of captured documents
- Workflow management
  - Will allow the management of standardized processes within and across all business entities
  - Will allow for the monitoring and review for all regulatory compliances
  - Will incorporate notifications, alerts and automated triggers to drive business processes and interfaces with internal and external entities
- System dashboards
  - Will allow all levels of management the ability to quickly monitor key business indicators through graphical data representation
  - Will provide the ability for authorized individuals to create customized views of data for analytical purposes
- Standardized and ad hoc information reporting
  - Will allow for the normalization of parameters for standardized reports
  - Will provide a reporting structure that allows reconciliation of all summary reports to supporting detail reports
  - Will present information to authorized individuals in a variety of formats through ad hoc queries and graphical reviews
- Automated interfaces
  - Will allow seamless collaboration with external business partners to ensure the timeliness and accuracy of shared information
  - Will utilize industry standard formats for the exchange of information in a secure manner
  - Will minimize manual interventions to reduce errors in the data exchanged with external entities



- Will provide a foundation for judicious responding to new and future interface requirements with current and future partners



- Audit trail functionality
  - Will provide the ability to track the details of all events that occur within the system including any addition, change or deletion of data
  - Will improve individual accountability, allows for reconstruction and verification of events and assist in analysis
  
- Fiscal controls
  - Will provide role-based security to ensure adequate and auditable separation of duties
  - Will be able to maximize the claims reimbursement by the use of integrated business rules, proper fiscal controls and financial accountability
  - Will be able to accurately report with complete transparency of the consolidated portfolio of accounts
  
- Microsoft Office and SharePoint compatibility
  - Will maximize the State's investment in Microsoft Office applications by integrating these products into the system for alternative views of system information
  - Will dynamically integrate with Microsoft SharePoint to allow the leveraging of document management functionality
  - Will use Microsoft Office business intelligence features to support statistical analysis and trending

### **Constraints**

Constraints are restrictions or limitations under which the Project Director must execute the project pertaining to people, money, time, and/or equipment. It is the Project Director's role to balance these constraints with available resources in order to ensure project success.

This project is constrained by the following factors:

- Limited to the funds approved by the Department of Finance and Administration
- Restrained by the fact that existing technical and business resources are currently allocated to other critical roles within the organization
- Dependent on the procurement of third party contract services for the configuration and implementation of the solution
- Must observe the rules of all pertinent regulatory agencies (CMS, Legislative, Judicial)
- All technology solutions implemented during this project must comply with State standards



- There is a single point of interface with TennCare which will affect the approach to implementation of the solution
- Providers across the State must have simultaneous access to identical functionality
- Solution access and response time will be dependent upon the characteristics of the State network
- Non-State users need online real time accessibility to portions of this solution
- Security must limit access to information base upon roles and responsibilities
- The system must satisfy all HIPAA requirements

### **Assumptions**

In the development of the project charter, the Project Team has identified the following assumptions under which the project is defined.

- The solution will be configured to best support the Department's future state
- The Department will reengineer its processes to align with the new solution
- The solution will be based upon the Microsoft Dynamics platform
- The project and the solution will have continuous support from DIDD leadership throughout the project
- There will be sufficient DIDD technical staff to gain adequate knowledge of and support of the solution after implementation
- Policy staff will have the resources and authority to reengineer the procedures documentation to align with the solution
- This project will be the number one priority within DIDD until its completion
- This solution must be hosted within the State's data centers
- This project will have full support of the service providers engaged by DIDD
- The implementer will meet DIDD's expectations within the project budget

### **Preliminary Scope Statement**

Project Titan will focus on the design, configuration, testing and delivery of a business solution that addresses accurate and immediate data collection, secured data visibility, reporting from a central data repository and transaction auditability for DIDD's three programmatic areas: Financial Management, Planning and Protection from Harm. The solution will provide the foundation for improved business processes, efficient and effective use of resources and a growth path for future DIDD initiatives. All project work will be independent of daily and ongoing operations. This project will conclude when the final report is submitted within thirty (30) days after the defined solution is tested and



**ATTACHMENT E**

deployed across the DIDD organization, all technical documentation is completed and all deliverables have been signed off by the Project Director, the IT Director and Project Executive Sponsor.



## RISKS

All projects have risks that can threaten their successes. Project risks are identified and assessed and appropriate responses are determined throughout the project. The Risk Management plan will address the methodology the project will employ to decrease the probability and impact of risks. The risks addressed in this section are risks that were identified during the initiation of the project. The chart below exhibits the risks identified by the Project Team, their probabilities and their impact.

Risk Identification			Qualitative Rating			
Risk ID	Risk Category	Risk Identification	Probability (1-5)	Impact (1-5)	Risk Score (P x I)	Risk Ranking
1	Project Initiation	Inability to attain approval to proceed with the project	3	5	15	1
2	Schedule	Time required for procuring the platform implementation vendor	3	4	12	2
3	Scope	Lack of agreement or level of the detail of the requirements for this project	3	4	12	3
4	Human Resources	Lack of DIDD business and technical resource availability throughout the project	3	4	12	4
5	Budget	Funding of project less than what is needed to complete project within scope	1	5	5	5
6	Human Resources	DIDD will not have complete support from all providers	2	2	4	8
7	Scope	Unauthorized scope change	1	4	4	6
8	Scope	Staff and providers not complying with business reengineering or process changes	3	1	3	9
9	Human Resources	Turnover in project leadership positions	1	4	4	7



## PROJECT DELIVERABLES

There are four (4) deliverable categories that must be provided at the end of Project Titan by the Project Team. All deliverables will be the result of the effort and collaboration of the stakeholders, vendors and project management. There will be a formal acceptance process for these deliverables. These deliverable categories are:

- An operational solution that can be readily managed by the technical and business resources of DIDD and the technical resources of OIR
- Adequate training to DIDD staff, OIR staff and service providers to allow the effective uses and management of the solution
- Complete technical and user documentation describing how to operate and maintain the solution
- Complete project documentation that reflects the planning, execution and completion of the project

## SUMMARY MILESTONE SCHEDULE

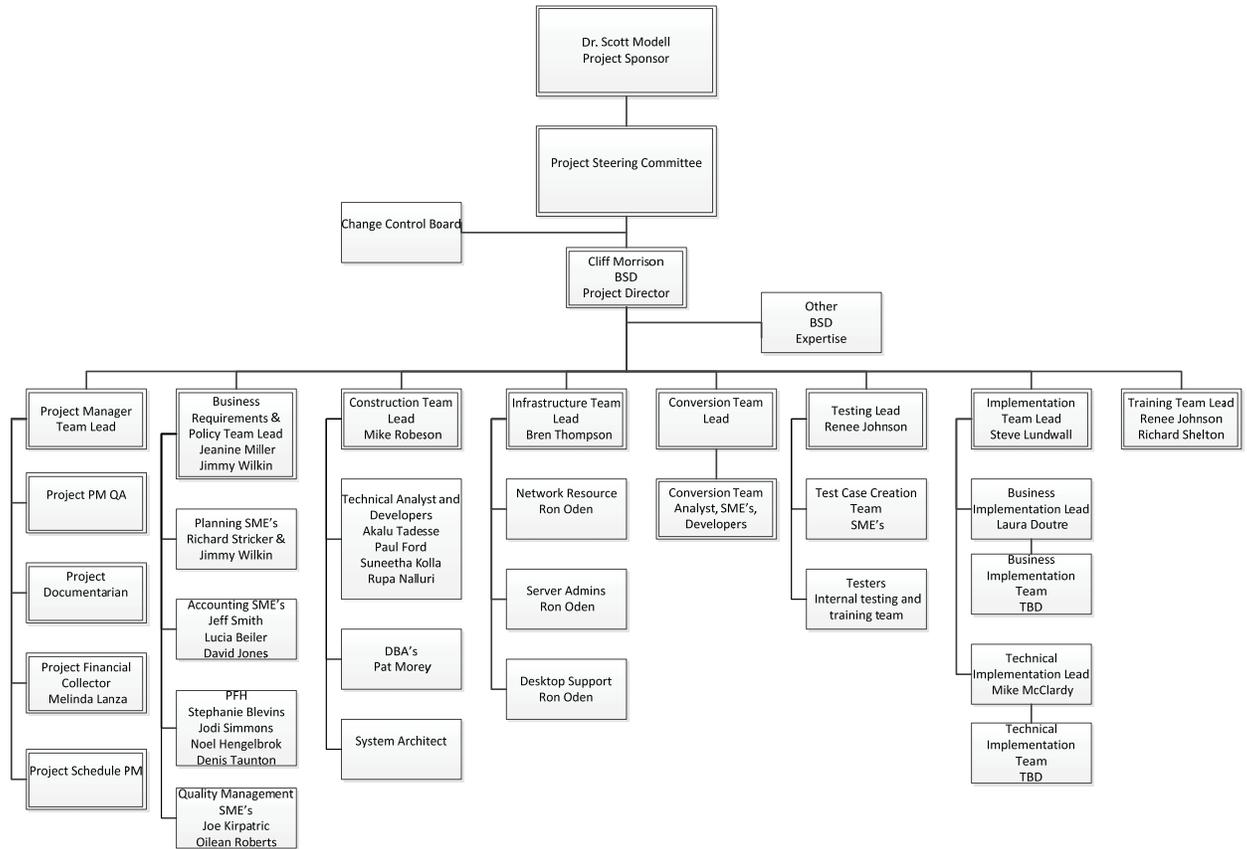
The project Summary Milestone Schedule is presented below. As requirements are more clearly defined this schedule may be modified. Any changes will be communicated through project status meetings by the Project Manager.

<b>Summary Milestone Schedule – List key project milestones relative to project start.</b>		
<b>Project Milestone</b>	<b>Target Date</b>	<b>Completion Date</b>
• Project Pre-initiation Start	03/05/2012	3/5/2012
• Project Initiation Documentation completed	05/14/2012	5/17/2012
• Project Documentation submitted to IT-ABC	05/15/2012	5/17/2012
• Presentation to IT-ABC	05/21/2012	5/21/2012
• Project Approval	06/08/2012	
• Platform Procurement complete	06/30/2012	
• Implementation Provider Procurement Complete	07/30/2012	
• Design and Development Phase begins	08/15/2012	
• Design and Development Phases complete	09/10/2012	
• Project Complete	03/15/2014	



## ORGANIZATION AND RESPONSIBILITIES

Below is the organizational chart for the project, followed by a description of the roles and responsibilities for each position.



## PROJECT SPONSOR

The Project Sponsors will provide overall guidance to the project and provide senior-management direction as needed. Specifics of the role include:

- Actively champion the project and monitor project progress
- Maintain thorough understanding of the project
- Provide senior-level support and guidance
- Assist in removing obstacles to success
- Approve changes to project scope, timing, budget, and charter, as appropriate
- Empower the Project Team to make decisions
- Make strategic-level decisions and resolve issues in a timely manner



Project Sponsors are:

Name	Role
Dr. Scott Modell	Executive Project Sponsor
Commissioner Jim Henry	Commissioner of DIDD
Commissioner Mark Emkes	Commissioner of F&A

## PROJECT DIRECTOR

### Assigned Project Director

The assigned Project Director for Project Titan is Cliff Morrison.

### Role

The Project Titan Director is the person responsible for developing, in conjunction with the Project Sponsor, a definition of the project. The Project Director then ensures that the project is delivered on time, within budget and to the required quality standard. This person ensures the project is effectively resourced and manages relationships with a wide range of groups, including all project contributors.

### Responsibilities

The Project Director is responsible for managing the work of the project, allocating and utilizing resources in an efficient manner, managing vendor contracts, and maintaining a cooperative, motivated and successful team. The responsibilities of the Project Director include the following:

Recruiting project staff and consultants

Managing and leading the Project Team

Managing co-ordination of the partners and working groups engaged in project work

Detailed project planning and control including:

- Developing and maintaining a detailed project plan
- Managing project deliverables in line with the project plan
- Recording and managing project issues and escalating where necessary
- Resolving cross-functional issues at project level
- Managing project scope and change control and escalating issues where necessary



- Monitoring project progress and performance
- Providing status reports to the Project Sponsor(s)
- Managing project training within the defined budget
- Liaison with, and updates progress to, project steering board/senior management
- Managing project evaluation and dissemination activities
- Final approval of the design specification

### PROJECT STEERING COMMITTEE

Project Steering Committee members are any persons or groups who are to provide overall guidance as needed to assure that the program/project meets its goals and objectives. This committee is comprised of Executive and Business Sponsors and designated stakeholders representing the affected organizational units.

#### Responsibilities

- Review and recommend approval of program/project deliverables
  - Resolve issues or assist with issue resolution when escalation is required
  - Assist with risk mitigation
  - Provide direction on major decisions during project execution, such as change requests, trade-offs between cost/time/scope, and resource-availability conflicts
- Key Project Steering Committee members are:

Name	Role
Dr. Scott Modell	Executive Project Sponsor, Deputy Commissioner, Office of Policy & Innovation
Debbie Payne	Deputy Commissioner, Office of Program Operations
Dr. Tom Cheetham	Director, Office of Health Services
Pat Nichols	Assistant Commissioner, Quality Management
Russell Nicoll	Director, Information Technology
Lance Iverson	Assistant Commissioner, Fiscal & Administrative Services
Lee Vestal	Director, Risk Management
Theresa Sloan	Legal Counsel, Regulatory Affairs



Name	Role
Stephanie Dedmon	BSD Director
Jamie Etheridge	OIR
TDB	TennCare
Mike Dedmon	Budget Director, Finance & Administration

## PROJECT STAKEHOLDERS

Project Stakeholders are any persons or groups who have interests which may be positively or negatively impacted by the performance or completion of the project. The Key Project Stakeholders identified for Project Titan are actively involved within the project and as a result may exert influence over the project's objectives and outcomes. To account for stakeholder involvement, project deliverables shall require stakeholder review and approval as appropriate.

Key Project Stakeholders are:

Name	Role
Richard Strecker	Planning (Case Management, Intake)
Annette Caldwell-Binkley	Planning (Case Management, Intake)
Courtney Kelly	Planning (Case Management, Service Delivery, Plans Review)
Barbara DeBerry	Planning (Service Delivery, Plans Review)
Lucia Beiler	Planning (Case Management), Accounting (Financials)
Carol Scott	Planning (Case Management)
Linda Maurice	Planning (Provider Recruitment)



Name	Role
Richard Shelton	Planning (Provider Recruitment)
Luke Queen	Planning (Service Delivery)
Dr. Stacey Dixon	Planning (Service Delivery)
C.J. McMorran	Planning (Service Delivery)
John Craven	Planning (Service Delivery)
Diane Brightwell	Planning (Service Delivery)
Julie Huber	Planning (Service Delivery)
Jeff Smith	Accounting (Financials)
Lee Vestal	Accounting (Financials), Quality Management (Compliance)
Michelle Jernigan, TennCare	Accounting (Financials)
Ken Barker, TennCare	Accounting (Financials)
Janie Warren	Accounting (Financials)
Pat Nichols	Quality Management (Compliance)
Joe Kirkpatrick	Quality Management (Compliance)
Jeff Davis	Quality Management (Compliance)
Kelly McCain	Quality Management (Compliance)
Stephanie Blevins	Quality Management (Protection from Harm)



Name	Role
Jodi Simmons	Quality Management (Protection from Harm)
Noel Hengelbrok	Quality Management (Protection from Harm)
Jeanine Miller	Quality Management (Policy)
Laura Doutre	Quality Management (Policy)
Kim Dean	Quality Management (Policy)
Michelle Ojima	Quality Management (Policy)
Russell Nicoll	Technology
TBD	Technology

## PROJECT TEAM

The Project Titan team will provide the day-to-day operation of the project and will:

- Serve as full-time participants on the project
- Participate/lead specific project tasks in accordance with the project plan
- Facilitate work sessions and conduct interviews, as appropriate
- Ensure adequate project documentation is created and maintained
- Perform development of assigned deliverables, and ensure deliverables are completed on schedule
- Actively participate in developing project work products, refining business processes, and in developing, implementing and testing system requirements
- Anticipate problems proactively and make recommendations for improvements
- Resolve issues in a timely manner per the project issue escalation policy
- Actively participate in Project Team meetings and status reporting activities
- Review project deliverables in accordance with deliverable review process



## Project Team Staffing Estimate

Project Role	Participation Estimate
BSD Project Director	1
Agency Project Manager	5
Business Requirements Team Manager	2
Planning Business Requirements Team Lead	1
Financial Business Requirements Team Lead	1
Protection From Harm Business Requirements Team Lead	1
Quality Assurance Requirements Team Lead	1
Construction Team Lead	1
Infrastructure Team Lead	1
Conversion Team Lead	1
OIR Project Manager	1
Testing Team Lead	1
Implementation Team Lead	1
Training Team Lead	1
Subject Matter Experts (Business)	20
Technical Experts	7
Business Analyst	7

**Participation Estimate:** The estimated number of FTEs who will serve on the project within the given role.



### PROJECT APPROVAL REQUIREMENTS

Success for Project Titan will be achieved when a fully tested solution and all technical user and user training is fully deployed throughout the Department of Intellectual and Developmental Disabilities within the time and cost constraints indicated in this charter. Success will be determined by the Project Sponsor, Dr. Scott Modell, who will also authorize completion of the project.

### AUTHORIZATION

Approved by:

	Date: _____
Cliff Morrison Project Director	

	Date: _____
Scott Modell Project Executive Sponsor	

	Date: _____
Russell Nicoll Project Technical Sponsor	



## Glossary

**Center for Medicare and Medicaid Services (CMS)**- shall mean the United States federal agency which administers Medicare, Medicaid, and the Children's Health Insurance Program.

**Earned Value Tool (EV)**- shall mean a business intelligence tool which supports the management's ability to track the progress of the project.

**Health Insurance Portability and Accountability Act (HIPAA)**- shall mean a federal law amended in 1996 that pertains to a person's right to have personal health records maintained in a confidential manner.

**Individual Support Plan (ISP)**- shall mean a person-centered document that provides an individualized, comprehensive description of the person supported as well as guidance for achieving unique outcomes that are important to the person in achieving a good quality of life in the setting in which they reside.

**Intermediate Care Facility (ICF)**-shall mean a licensed facility approved for Medicaid vendor reimbursement that provides specialized services for individuals with intellectual disabilities or related conditions and that complies with current federal standards and certification requirements for ICF/ID's.

**Office for Information Resources (OIR)**-shall mean a division of the Department of Finance and Administration which provides direction, planning, resources, execution and coordination in managing the information systems needs of the State of Tennessee.

**Person Centered Practices/Person Centered Services**- shall mean a process which is focused on the person who receives or will receive services in terms of who they are, what they want in life, and how their goals may be accomplished.

**Person Served**- shall mean an individual who is receiving services or has applied for services, because the person has an intellectual or developmental disability.

**Protection from Harm (PFH)**- shall mean a division of the Department of Intellectual and Developmental Disabilities which assures the protection and safety of persons served.

**Provider or Agency**- shall mean an agency who has been approved by DIDD to provide one or more HCBS waiver services and may include state-funded services.

**Requirements Traceability Matrix (RTM)**- shall mean a tool which ensures the solution will match DIDD's business requirements.



**Services-** shall mean a DIDD approved employment, day or residential program, therapy, case management and/or support coordination for individuals with intellectual or developmental disabilities.

**Stakeholder-**shall mean an entity outside DIDD that is affected by DIDD policies

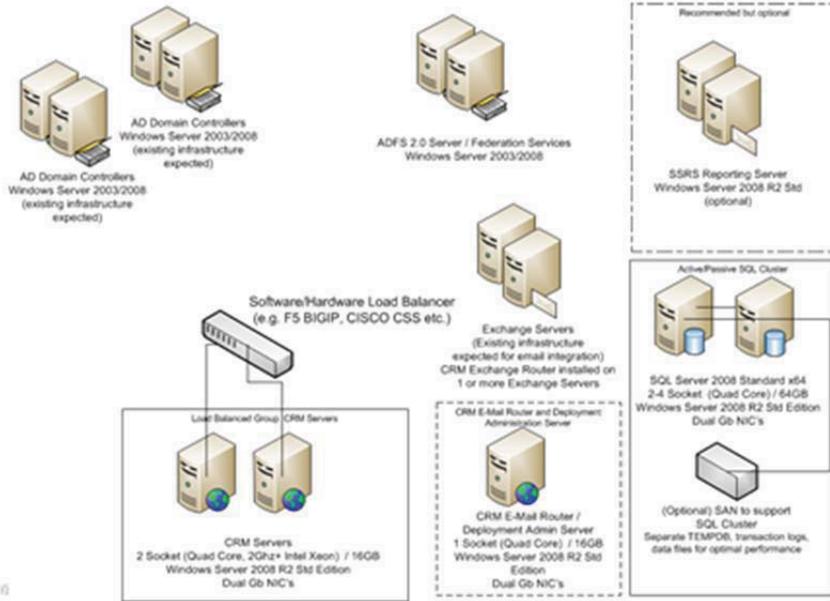
**TennCare-**shall mean the single State Medicaid Agency responsible for the administration of the State's Medicaid Program.

**User Acceptance Testing (UAT)-** shall mean a process for the subject matter experts to review and test the business solution to ensure it is successful.



# Proposed Production Environment for DIDD Solution

## Production – Baseline



Microsoft Confidential



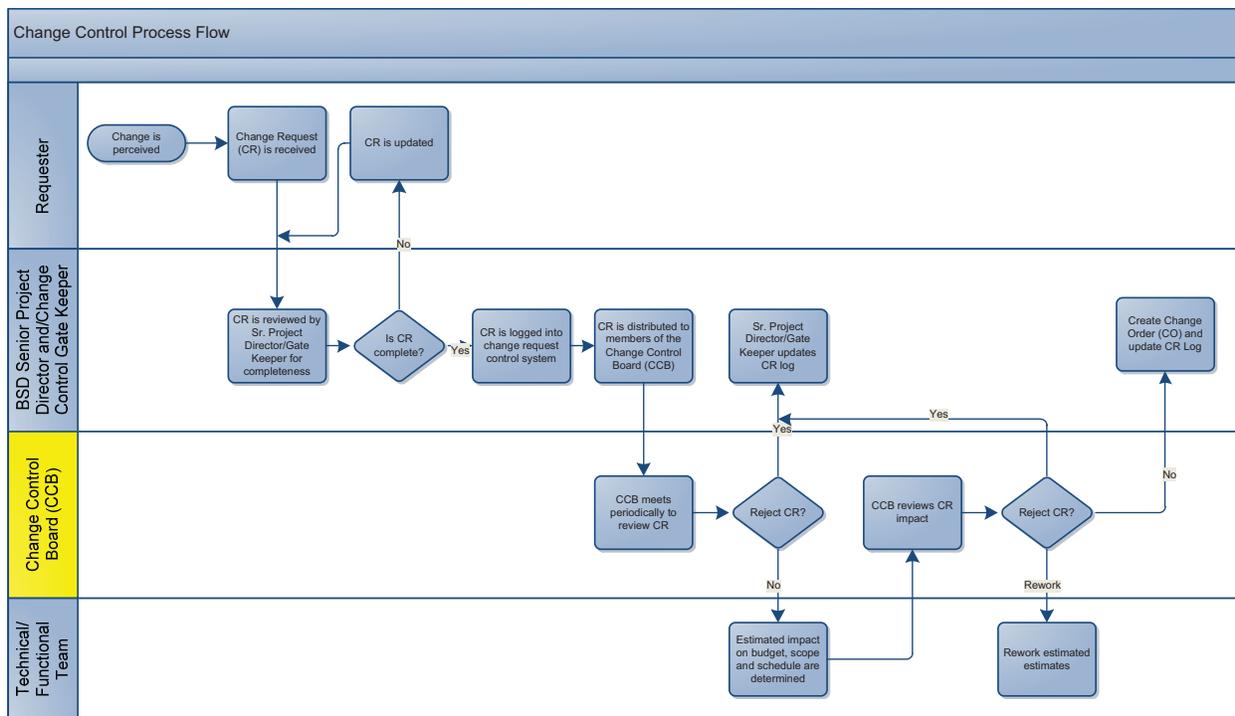
### Introduction

#### Change Control

The Change Management Process is undertaken to ensure that each change introduced to the project environment is appropriately defined, evaluated and approved prior to implementation. Change Management will be introduced to this project through the implementation of five key processes:

- The submission and receipt of change requests
  - The review and logging of change requests
  - The determination of the feasibility of change requests
  - The approval of change requests
- The implementation and closure of change requests.

The following swim lane diagram describes the roles, processes and procedures to be undertaken to initiate, implement and review the effects of changes within the project.



### Change Management Process

#### Identify and Submit Change Request

This process provides the ability for any member of the project team to submit a request for a change to the project. The Change Requester:



- Identifies a requirement for change to any aspect of the project (e.g. scope, deliverables, timescales and organization)
- Completes a Change Request form (CR) and distributes the form to the BSD Senior Project Director. The CR summarizes the change:
  - Description
  - Reasons/Goals for changes
  - Recommendations
  - Impacts (Cost, Scope, Schedule, and/or Quality)
  - Solution
  - Disposition (Approve, Reject, Defer)

### **Review Change Request**

The Sr. Project Director/Change reviews the CR and determines whether or not additional information is required for the Change Control Board to assess the full impact of the change to the project time, scope, cost and/or quality. The decision will be based on factors, such as:

- Number of change options presented
- Feasibility and benefits of the change
- Complexity and/or difficulty of the change options requested
- Scale of the change solutions proposed.

The Sr. Project Director will record the CR details in the Change Log to track the status of the change request.

### **Approve Change Request**

The Sr. Project Director will forward the Change Request Form and any supporting documentation to the Change Control Board (CCB) for review and final approval. The CCB will determine the feasibility of this change by examining factors, such as:

- Risk to the project in implementing/not implementing the change
- Impact on the project in implementing the change (time, resources, finance, quality).

After a formal review, the CCB may:

- Approve the change as requested
- Reject the change
- Request more information related to the change.



# State of Tennessee Enterprise Architecture

---

## Technology Architecture

### Standard Product Components

Submitted on September 21, 2011 to:  
State of Tennessee Office for Information Resources Executive Leadership Team

Executive Sponsor:  
Mark Bengel  
State of Tennessee Chief Information Officer  
Department of Finance and Administration  
Office for Information Resources



# Technology Architecture Framework

The State of Tennessee Information Systems Council (ISC) has assigned the responsibility for the development of the State's Technology Architecture to the Office for Information Resources. The Technology Architecture is an integral part of the Enterprise Architecture and is the official publication documenting information technology products and standards.

Technology Architecture Standards are applicable to all state agencies (e.g., departments, boards, commissions, offices, and institutions of the state) and extend to vendors contracted to work for state agencies. Exceptions to Enterprise Architecture standards are governed by the Waiver/Exception process (see Appendix A).

The Technology Architecture establishes technical requirements which govern the planning, acquisition, use, and management of information technology resources. It organizes, classifies, and categorizes them in an orderly framework of Domains, Disciplines and Technology Areas. The concept of domains, disciplines and technology areas are aligned with the National Association of State Chief Information Officers (NASCIO) Enterprise Architecture Toolkit.



# Technology Architecture Domains

The Technology Architecture Domains are listed below with a brief description.

## *Application*

The Application Domain documents the languages, tools and utilities to design, build, deploy, operate and maintain the State's applications.

## *Collaboration*

The Collaboration Domain identifies standards and components that facilitate interaction of the workforce and promote group productivity.

## *Data*

The Data Domain addresses technology requirements for the storage and management of critical State data in electronic form.

## *Information*

The Information Domain addresses technology requirements for development and maintenance of areas requiring significant multi-agency coordination in the context of enterprise data and resource management.

## *Network*

The Network Domain documents the technology required to support the movement of electronic information and to support the voice, data and video infrastructures.

## *Platform*

The Platform Domain identifies technology hardware platforms and the related operating systems to support the current and future business requirements, standardizes configurations and defines host communications.

## *Security*

The Security Domain provides for integrating security services, mechanisms, objects and management functions, across multiple hardware and software platforms and networks.

## *Systems Management*

The Systems Management Domain defines the framework for efficient and effective management of the State's information processing environment, including monitoring and management of peripheral devices, processes for production systems, and the capability to recover the production environment in part or in whole.



# Technology Architecture Product Phases

The Technology Architecture Products component facilitates planning by identifying a lifecycle phase for each standard product. The phases are listed below with a brief description.

## *Emerging*

Technologies that, while possibly accepted as well utilized throughout the industry, are new to the enterprise. It is generally understood that emerging technologies be considered carefully before implementing in the enterprise-wide architecture. It is therefore recommended that, for initial implementation, emerging technologies be limited to smaller, non-mission-critical projects until it is proven that they can be integrated successfully into the existing enterprise architecture.

## *Current*

Technologies that are the current standard for use within the enterprise, and tested and generally accepted as standard within the industry. These items comply with or support the principles listed for the discipline.

## *Twilight*

Technologies being phased out by the enterprise but not yet having an established end date.

## *Obsolete*

Technologies that have been phased out and cannot be used within the organization past a specific date.



# Technology Architecture Product Standards

## Domain: Application

### Discipline: Application Access

#### Technology Area: Application Server

IBM Websphere Application Server	Current
Microsoft .NET	Current
Oracle Application Server 10g	Current
Oracle Application Server 9i	Twilight
Red Hat JBoss	Current

#### Technology Area: Web Browser

Internet Explorer 5	Twilight
Internet Explorer 6	Twilight
Internet Explorer 7	Current
Internet Explorer 8	Current
Internet Explorer 9	Emerging
Netscape	Obsolete

#### Technology Area: Web Server

IBM HTTP Server	Current
Microsoft Internet Information Server	Current
Netscape	Twilight
Open Source Apache Web Server 2.0 or higher	Current
Oracle Apache	Current

### Discipline: Application Configuration Management

#### Technology Area: Application Change Management

Serena PVCS Teamtrack	Current
-----------------------	---------



# Technology Architecture Product Standards

## Technology Area: Application Release Management

---

Serena PVCS Builder	Twilight
---------------------	----------

## Technology Area: Application Version Control

---

Librarian Change Control Facility	Current
Oracle Software Configuration Management	Emerging
Serena PVCS Version Manager	Current
Subversion	Current
Visual SourceSafe	Current

## Discipline: Application Development

---

### Technology Area: Languages

---

ADF	Twilight
C#	Current
COBOL for z/OS and OS/390	Current
FoxPro	Twilight
Java 1.4.2	Current
Microsoft VB .NET	Current
PowerBuilder	Twilight
Rexx	Current
Visual Basic	Twilight

### Technology Area: Tools & Utilities

---

3270 Superopt/CICS	Current
Abend-Aid	Current
Batch Terminal Simulator (BTS)	Current
CA Easytrieve Plus	Current
CA-Copycat	Current



# Technology Architecture Product Standards

CA-Disk	Current
CA-Ops/MVS	Current
Cool:Gen	Twilight
DB2 Tools for IMS	Current
Delta/IMS	Current
DL/2	Current
EMC Catalog Solution	Current
Filesave/RCS	Current
Finalist	Current
Finalist (Cross Check)	Current
HourGlass	Current
IBM Document Composition Facility (DCF)	Current
IBM Move for DB2	Current
IMS Connect	Current
Install/1	Current
I-Way EDS	Current
Mail Stream (Mailer's Choice)	Current
Maxm Reorg	Current
NDoc	Current
Oracle Designer 10g	Twilight
Oracle Designer 4.5	Obsolete
Oracle Designer 6i	Obsolete
Oracle Designer 9i	Twilight
Oracle Discoverer 10g	Twilight
Oracle Discoverer 4.1	Twilight
Oracle Discoverer 9i	Twilight
Oracle Forms Developer 10g	Twilight



# Technology Architecture Product Standards

Oracle Forms Developer 4.5	Obsolete
Oracle Forms Developer 6i	Obsolete
Oracle Forms Developer 9i	Twilight
Oracle Jdeveloper 10g	Twilight
Oracle Jdeveloper 9i	Twilight
Oracle Reports Developer 10g	Twilight
Oracle Reports Developer 4.5	Obsolete
Oracle Reports Developer 6i	Obsolete
Oracle Reports Developer 9i	Twilight
Performance Essentials	Current
PkZip for Mainframe	Current
Quick Index	Current
QuickRef for MVS	Current
RACF Toolkit	Current
SAS Foundation	Current
SSA Name3	Current
Syncsort	Current
TELON	Twilight
ThruputManager	Current
TMON TCPIP	Current
UltraOpt	Current
VB Commenter	Twilight
Viasoft	Current

## **Technology Area: Web Application Development Tools**

Eclipse IDE for Java Developers	Current
Microsoft Dynamics CRM	Current



# Technology Architecture Product Standards

Oracle Internet Developer Suite 10g	Twilight
Oracle Internet Developer Suite 9i	Twilight
Rational Application Developer (RAD) for WebSphere	Current
Rational Software Architect	Current
Visual Studio .NET 2005	Twilight
Visual Studio .NET 2008	Current

## Technology Area: Web Graphical User Interface Development Tools

Jacada Interface Server	Current
Oracle Internet Developer Suite 10g	Twilight
Oracle Internet Developer Suite 9i	Twilight
WebSphere Host Access Transformation Services (HATS)	Current

## Discipline: Application Testing

### Technology Area: Functional Testing

Compuware Hiperstation Plus	Current
Compuware QACenter 3270 Hiperstation	Current
Micro Focus QADirector	Current
Micro Focus TestPartner	Current

### Technology Area: Performance Testing

Compuware Application Vantage	Current
Micro Focus QALoad	Current

### Technology Area: Test Data Generation

Compuware File-AID/CS	Current
-----------------------	---------

### Technology Area: Tuning/Development

Micro Focus DevPartner	Current
------------------------	---------



# Technology Architecture Product Standards

## Discipline: Output Management

---

### Technology Area: Output Management

---

DataWare-CD - Luminex	Current
Document Direct for the Internet + (formerly Document Direct)	Current
DRS	Current
IBM Advanced Function Printing	Current
InfoPrint Server	Current
Monarch	Current
TriTek Output Express	Current
View Direct (formerly InfoPac)	Current
VMCFC	Current
VPS	Current



# Technology Architecture Product Standards

## Domain: Collaboration

### Discipline: Collaboration Tools

#### Technology Area: Desktop Publishing

Adobe PageMaker	Current
Microsoft Publisher 2000 and 2002	Twilight
Microsoft Publisher 2003 and 2007	Current
Microsoft Visio 2002	Twilight
Microsoft Visio 2003 and 2007	Current

#### Technology Area: Office Automation

Microsoft Office 2003 and 2007	Current
Microsoft Office 2010	Current
Microsoft Office 97	Obsolete
Microsoft Office XP	Twilight

#### Technology Area: Project Management

Microsoft Project 2000	Obsolete
Microsoft Project 2003 and 2007	Current
Microsoft Project Server 2000	Obsolete
Microsoft Project Server 2003 and 2007	Current
Project Workbench	Obsolete

#### Technology Area: Spreadsheet

Lotus 1-2-3	Obsolete
Microsoft Excel 2000	Twilight
Microsoft Excel 2003	Current
Microsoft Excel 2007	Current



# Technology Architecture Product Standards

Microsoft Excel XP	Twilight
--------------------	----------

## Technology Area: Team Collaboration

---

Microsoft Office SharePoint Server 2007	Current
Microsoft Office SharePoint Server 2010	Emerging
Windows SharePoint Services 3.0	Current

## Technology Area: Word Processing

---

Microsoft Word 2000	Twilight
Microsoft Word 2003	Current
Microsoft Word 2007	Current
Microsoft Word 2010	Current
Microsoft Word XP	Twilight
Word Perfect	Twilight

## Discipline: Directory Services

---

### Technology Area: Directory Services

---

eDirectory (formerly NDS Directory)	Twilight
eTrust IdentityMinder eProvision (formerly Netegrity eProvision)	Obsolete
Microsoft Active Directory	Current
Resource Access Control Facility (RACF)	Current

## Discipline: Document Lifecycle Management

---

### Technology Area: Automated Data Capture

---

Datacap Taskmaster	Current
IBM FileNET Capture Desktop 4.x	Twilight
IBM FileNET Capture Desktop 5.x	Current
IBM FileNET Capture Pro 4.x	Twilight
IBM FileNET Capture Pro 5.x	Current



# Technology Architecture Product Standards

Lexmark	Current
TriTek CapturePlus	Current
Verity (formerly CARDIFF TELEForm Information Capture)	Twilight

## Technology Area: Document Imaging

---

IBM FileNET Content Services	Twilight
IBM FileNET Image Services	Twilight

## Technology Area: Document Management

---

IBM FileNET Content Manager 3.x	Twilight
IBM FileNET Content Manager 4.x	Current
IBM FileNET Image Manager 2.x	Twilight
IBM FileNET Image Manager 3.5.2	Twilight

## Technology Area: Workflow

---

eProcess Services	Twilight
IBM FileNet Business Process Manager 2.x	Twilight
IBM FileNet Business Process Manager 3.5.2	Twilight
IBM FileNET Business Process Manager 4.5	Current
TriTek Trans@ction eXpress 4.5	Current

## Discipline: Electronic Mail

---

### Technology Area: Electronic Mail

---

Blackberry Enterprise Server 4	Twilight
Blackberry Enterprise Server 4.1	Current
Blackberry Enterprise Server 5.0	Current
FaxWare	Current
Microsoft Exchange Server 2007	Twilight
Microsoft Exchange Server 2010	Current



# Technology Architecture Product Standards

Novell GroupWise Client 6	Obsolete
Novell GroupWise Client 6.5.1	Current
Novell GroupWise Server 6	Obsolete
Novell GroupWise Server 7	Twilight
Novell GroupWise Server 8.02	Current

## Technology Area: Gateway

---

GroupWise Internet Agent (GWIA)	Current
Secure Mail (IronMail)	Current
SendMail (SMTP)	Current
SMTP Compliance Component	Current
Symantec AntiVirus	Current

## Technology Area: List Management Software

---

LISTSERV	Current
----------	---------

## Discipline: Mobile Devices

---

### Technology Area: Data Synchronization

---

Intellisync	Obsolete
-------------	----------

### Technology Area: Handheld Devices

---

Pocket PC 2002	Obsolete
RIM Blackberry (Data & Push-to-Talk)	Current
RIM BlackBerry (Data Only)	Current
RIM Blackberry (Data Telephony)	Current
Windows Mobile 2003 for Pocket PC	Twilight

## Discipline: Web Publishing

---

### Technology Area: Web Publishing

---



# Technology Architecture Product Standards

Adobe Acrobat	Current
Adobe Contribute	Current
Adobe Dreamweaver	Current
Adobe Fireworks	Current
Adobe Flash	Current
FrontPage	Obsolete



# Technology Architecture Product Standards

## Domain: Data

### Discipline: Data Access

#### Technology Area: Database Middleware

DB2 Connect Client	Current
DL/2	Current
Open Text LiveLink ECM (formerly Hummingbird BI/Query)	Twilight

### Discipline: Data Management

#### Technology Area: Data Backup/Recovery

Various DB utilities	Current
----------------------	---------

#### Technology Area: Data Movement

Connect: Direct	Current
FTP	Current
IBM Move for DB2	Current
IMS CDC	Current
MVS/Expedite	Current
Oracle (64-bit) 11g	Current
Oracle Enterprise Grid Control	Current
Oracle Enterprise Manager Database Control	Current
Quest Toad	Current
RC/Migrator for DB2 for z/OS 11.5	Current
RC/Migrator for DB2 for z/OS 6.1.6	Obsolete
RC/Update for DB2 for z/OS 11.5	Current
RC/Update for DB2 for z/OS 6.1.6	Obsolete
Secure FTP (SFTP)	Current
SQL Server Management Studio	Current



# Technology Architecture Product Standards

XCOM Current

**Technology Area: Data Quality**

---

**Technology Area: Data Translator**

---

EC Gateway Current

ECMap Current

ECRTP Current

EDI Server Current

**Technology Area: Extract, Transform, and Load**

---

Talend Open Studio Current

**Technology Area: Repository for Data Management**

---

**Discipline: Database Storage**

---

**Technology Area: Database Change Management**

---

RC/Migrator for DB2 for z/OS 11.5 Current

RC/Migrator for DB2 for z/OS 6.1.6 Obsolete

RC/Update for DB2 for z/OS 11.5 Current

RC/Update for DB2 for z/OS 6.1.6 Obsolete

**Technology Area: Database Management System**

---

Compress for IMS Current

DB2 Universal Database (UDB) for z/OS 7.1 Obsolete

DB2 Universal Database (UDB) for z/OS 8.1 Twilight

DB2 Universal Database (UDB) for z/OS 9 Current

DSIMS (IMS) 6.1.6 Current

FoxPro Twilight

IMS DB for OS/390 Twilight



# Technology Architecture Product Standards

Informix	Twilight
Microsoft Access	Current
Microsoft SQL Server 2000	Twilight
Microsoft SQL Server 2005	Current
Microsoft SQL Server 2008	Current
Oracle (32-bit) 10g	Current
Oracle (32-bit) 11g	Current
Oracle (32-bit) 7.3.4	Obsolete
Oracle (32-bit) 8.0	Obsolete
Oracle (32-bit) 8i	Obsolete
Oracle (32-bit) 9i	Obsolete
Oracle (64-bit) 10g	Current
Oracle (64-bit) 11g	Current
Oracle (64-bit) 7.3.4	Obsolete
Oracle (64-bit) 8.0	Obsolete
Oracle (64-bit) 8i	Obsolete
Oracle (64-bit) 9i	Obsolete

## Technology Area: Database Monitoring

---

Database Analyzer (DB2) 11.5	Current
Database Analyzer (DB2) 2.6.6	Obsolete
Savant (for Oracle)	Current
The Monitor for DB2	Current
The Monitor for IMS (TMON/IMS)	Current

## Discipline: Database Structure

---

### Technology Area: Data Modeling/Database Design

---



# Technology Architecture Product Standards

CA Erwin Modeling Suite 4.1.4	Current
Oracle Designer 10g	Twilight
Oracle Designer 4.5	Obsolete
Oracle Designer 6i	Twilight
Oracle Designer 9i	Twilight
PowerDesigner (formerly Data Architect)	Current



# Technology Architecture Product Standards

## Domain: Information

### Discipline: Business Intelligence

#### Technology Area: Data Analysis

Microsoft SQL Server Analysis Services	Current
MicroStrategy Desktop	Current
MicroStrategy Desktop 7.5.3	Twilight
MicroStrategy Intelligence Server	Current
MicroStrategy Intelligence Server 7.5.3	Twilight
MicroStrategy Narrowcast Server	Current
MicroStrategy Narrowcast Server 7.5.3	Twilight
MicroStrategy Web Server	Current
MicroStrategy Web Server 7.5.3	Twilight
Oracle Discoverer 10g	Twilight
Oracle Discoverer 4.1	Twilight
Oracle Discoverer 9i	Twilight

#### Technology Area: Data Mining

#### Technology Area: Information Delivery

TriTek Report Data Exchange	Current
-----------------------------	---------

#### Technology Area: Query/Reporting

Base SAS	Current
Business Objects Crystal Reports Server 2008 v.11 (formerly Crystal Enterpr	Current
CA Easytrieve Plus	Current
Crystal Reports	Current
Datavantage	Current



# Technology Architecture Product Standards

File-Aid	Current
File-AID/IMS	Current
Microsoft SQL Server Reporting Services 2005	Current
Monarch	Current
Open Text LiveLink ECM (formerly Hummingbird BI/Query)	Twilight
Oracle Discoverer 10g	Twilight
Oracle Discoverer 4.1	Obsolete
Oracle Discoverer 9i	Twilight
Oracle Reports 10g	Current
Oracle Reports 4.5	Obsolete
Oracle Reports 6i	Twilight
Oracle Reports 9i	Obsolete
QMF 6.1	Current
RC/Update 6.1.6	Current
SAS Foundation v 9.1.3	Current
SAS Foundation v 9.2	Current
SAS/STAT	Current
SQR	Obsolete

## Discipline: Geographic Information Systems (GIS)

### Technology Area: Data Server

ArcGIS Engine 10	Emerging
ArcGIS Engine 9.2	Twilight
ArcGIS Engine 9.3	Current
ArcGIS Server 10	Emerging
ArcGIS Server 9.2	Twilight
ArcGIS Server 9.3	Current



# Technology Architecture Product Standards

ArcIMS	Current
ArcIMS 10	Emerging
ArcIMS 3.x	Obsolete
ArcIMS 8.x	Twilight
ArcIMS 9.2	Current
ArcIMS 9.3	Current
MapObjects	Twilight

## Technology Area: Desktop Client

---

ArcGIS Desktop 10.0	Emerging
ArcGIS Desktop 9.3	Current
ArcGIS Explorer	Current
ArcInfo 3.x	Obsolete
ArcInfo 8.x	Twilight
ArcInfo 9.2	Twilight
ArcView 9.2	Twilight

## Technology Area: PDA Client

---

ArcPad 10	Emerging
ArcPad 5.x	Obsolete
ArcPad 6.x	Twilight
ArcPad 7.1	Twilight
ArcPad 8	Current

## Discipline: Message Integration

---

### Technology Area: Message Integration

---



# Technology Architecture Product Standards

## Domain: Network

### Discipline: Cabling

#### Technology Area: LAN Cabling

Cat 5	Obsolete
Cat 6, Fiber Optic 62.5/125 Multimode	Twilight
Cat 6a	Current
Fiber Optic 50/125 Multimode	Current
Single Mode Fiber Full Spectrum	Current

#### Technology Area: SNA Cabling

Cat 6, 25-pin EIA	Twilight
Cat 7	Twilight
RG-62, Coaxial Cable	Obsolete

#### Technology Area: Video Cabling

Cat 6	Current
Cat 7	Twilight
RG-6 Coax, RG-11 Coax	Current

#### Technology Area: Voice Cabling

Cat 3	Obsolete
Cat 5	Obsolete
Cat 6	Current
Cat 7	Twilight

#### Technology Area: WAN Cabling



# Technology Architecture Product Standards

Cat 6, Fiber Optic 62.5/125 Multimode	Twilight
Cat 6a	Current
Fiber 50/125 Multimode Laser Optimized	Current
Fiber Optic Single Mode	Current
Single Mode Fiber Full Spectrum	Current

## Discipline: LAN

### Technology Area: Adaptors

Ethernet	Current
Token Ring	Obsolete

### Technology Area: File Access and Transfer Service

Attachmate Extra Enterprise 2000 (formerly Attachmate Extra)	Current
FTP	Current
XCOM	Current

### Technology Area: Hubs/Switches

Cisco	Current
Nortel	Current

### Technology Area: LAN Protocol

TCP/IP	Current
--------	---------

### Technology Area: Monitoring

Network Associates Sniffer Suite	Current
----------------------------------	---------

### Technology Area: Secure File Transfer Protocol and Service

### Technology Area: Wireless LAN

Aruba	Current
-------	---------



# Technology Architecture Product Standards

## Discipline: SNA

### Technology Area: SNA Backbone Transport

DACS Switches	Twilight
T1	Twilight
T3 Channels	Twilight

### Technology Area: SNA Protocol

DLSw	Twilight
SNA-SDLC	Twilight

## Discipline: Video

### Technology Area: CSU/DSU

Adtran	Obsolete
Paradyne	Obsolete

### Technology Area: Document Camera

Cannon	Twilight
Elmo	Current

### Technology Area: Modems

MultiTech	Obsolete
-----------	----------

### Technology Area: Telemedicine Peripherals

AMD	Current
-----	---------

### Technology Area: Video Bridge

Polycom	Twilight
Video Accord	Twilight
Vtel	Obsolete



# Technology Architecture Product Standards

## Technology Area: Video Circuit/Carrier

ISDN/BRI	Twilight
ISDN/PRI	Twilight
T-1	Current

## Technology Area: Video CODEC

Polycom	Twilight
Tandberg	Current

## Technology Area: Video Protocol

H.320	Twilight
H.323	Current

## Technology Area: Video Switches

Cisco	Current
Initia	Obsolete
Nortel	Current

## Discipline: Voice

### Technology Area: Business Lines

1FB	Current
-----	---------

### Technology Area: Commercial C/O Service

Centrex	Current
---------	---------

### Technology Area: IP Telephony

Cisco Unified Communications Solutions	Current
--	---------

### Technology Area: PBX Trunks

ISDN/PRI	Twilight
----------	----------



# Technology Architecture Product Standards

## Technology Area: Voice Backbone Transport

Electronic Tandem Network (ETN)	Twilight
---------------------------------	----------

## Discipline: WAN

### Technology Area: Network Monitoring/Management

Alteon	Current
Cisco Works 2000	Twilight
DDNS	Current
DHCP	Current
F5	Current
Juniper SRX Series	Current
MRTG	Current
NAT	Current
Remedy	Current
SNIPS	Current
Solarwinds Orion Network Configuration Manager	Current

### Technology Area: Routing Equipment

Cisco - all product lines	Current
Juniper SRX Series	Current

### Technology Area: WAN Carrier/Circuit

ATM	Twilight
DS1	Current
DS3, OC3	Current
DSL	Current
Frame Relay	Twilight
ISDN	Current



# Technology Architecture Product Standards

SMDS/CDS

Obsolete

## Technology Area: WAN Protocol

---

BGP

Current

IPX

Twilight

MPLS

Current

OSPF

Current

PPP

Current

TCP/IP

Current

## Technology Area: WAN URL Filtering

---

## Discipline: Wireless Data Tele-Communications

---

### Technology Area: Wireless Protocol

---

802.11A

Current

802.11B

Current

802.11G

Current

802.11I

Current

802.11N

Current

802.1X

Current

### Technology Area: Wireless Transport

---

2.4 GHz

Current

5 GHz

Current

5.8 GHz

Current



# Technology Architecture Product Standards

## Domain: Platform

### Discipline: Environments

#### Technology Area: Environment

### Discipline: Hardware

#### Technology Area: Hardware

IBM (zSeries compatible)	Current
Intel/AMD (formerly X86) (formerly Intel)	Current
Solaris SPARK	Current
Solaris SPARK 2.7	Twilight
Solaris SPARK 2.8	Twilight

### Discipline: Host Communications

#### Technology Area: Host Communications

ACF/NCP (Network Control Program)	Obsolete
ACF/VTAM (telecommunications access)	Current
Attachmate Extra Enterprise 2000 (formerly Attachmate Extra)	Current
Host on Demand (HOD) +	Twilight
Personal Communications (formerly IBM Personal Communications/3270 - RJE)	Obsolete
TCP/IP	Current
TN-3270 (formerly PC3270)	Current
XCOM	Current

### Discipline: Operating Systems

#### Technology Area: Application/Database Server Operating System



# Technology Architecture Product Standards

CITRIX	Current
Netware 6	Obsolete
Netware 6.5	Twilight
Netware Client 4.91 SP2	Current
Red Hat Linux 4.5	Twilight
Red Hat Linux 5	Current
Solaris SPARC compatible 2.10	Current
Solaris SPARC compatible 2.6	Twilight
Solaris SPARC compatible 2.7	Twilight
Solaris SPARC compatible 2.8	Twilight
Suse Linux Enterprise Server	Twilight
Vmware 3.02	Twilight
Vmware 3.5.1	Twilight
Vmware 4.1	Current
Windows 2000 Server	Twilight
Windows 2000 Workstation	Twilight
Windows 2003 Server R2	Current
Windows 2008 Server R2	Current
Windows 7	Current
Windows NT Server	Obsolete
Windows NT Workstation	Obsolete
Windows XP Professional SP2	Twilight
Windows XP Professional SP3	Current
z/OS 1.7	Current
z/OS 1.9	Emerging

## Technology Area: File Services

---



# Technology Architecture Product Standards

Netware 6	Obsolete
Netware 6.5	Twilight
Windows File Services	Current

## **Technology Area: Handheld Devices Operating Systems**

---

Pocket PC 2002	Obsolete
RIM Blackberry (Data & Push-to-Talk)	Current
RIM BlackBerry (Data Only)	Current
RIM Blackberry (Data Telephony)	Current
Windows Mobile 2003 for Pocket PC	Obsolete

## **Discipline: Platform Configuration**

---

### **Technology Area: Platform Configuration**

---



# Technology Architecture Product Standards

## Domain: Security

### Discipline: Access Control

#### Technology Area: Database

Local User Database	Current
---------------------	---------

#### Technology Area: System

Operating System Security	Current
---------------------------	---------

UNIX Operating System Security	Current
--------------------------------	---------

### Discipline: Authentication

#### Technology Area: Authentication Protocol

Kerberos	Current
----------	---------

#### Technology Area: Certificates

Entrust	Current
---------	---------

Microsoft Certificate Server	Current
------------------------------	---------

#### Technology Area: Mainframe

Resource Access Control Facility (RACF) Security	Current
--	---------

#### Technology Area: Multi-Factor Authentication

Entrust	Current
---------	---------

#### Technology Area: Public Key Encryption

DSA	Current
-----	---------

Rivest, Shamir, Adelman Algorithm (RSA)	Current
---	---------

#### Technology Area: Public Key Infrastructure

Entrust	Current
---------	---------



# Technology Architecture Product Standards

## Technology Area: Symmetric Key Encryption

---

Advanced Encryption Standard (AES)	Current
Triple Data Encryption Standard (DES) and (3DES)	Current

## Technology Area: VPN

---

Check Point VPN-1	Current
Cisco Secure Remote Access	Current
Juniper SRX Series	Current
Microsoft PPTP	Twilight

## Discipline: Authorization

---

### Technology Area: Directory

---

eDirectory (formerly NDS Directory)	Twilight
Microsoft Active Directory	Current
Oracle Internet Directory	Current

## Discipline: Compliance Policies

---

### Technology Area: Anti-Spam

---

Secure Computing CipherTrust IronMail	Current
---------------------------------------	---------

### Technology Area: Firewall

---

Check Point Firewall-1	Current
Cisco ASA	Current
Cisco PIX	Current
Juniper SRX Series	Current

### Technology Area: Intrusion Detection

---



# Technology Architecture Product Standards

Cisco MARS	Twilight
Cisco SIMS	Obsolete
Juniper IDP Series	Current
Juniper SRX Series	Current
Juniper STRM	Current
RealSecure	Current

## Technology Area: Log-in

---

Microsoft Windows Logon (formerly NT Logon)	Current
Power-on Passwords	Current
RC/Secure (DB2)	Current
Screen Saver with password	Current

## Technology Area: URL Filtering

---

Websense	Current
----------	---------

## Technology Area: Virus Protection

---

Symantec AntiVirus	Current
--------------------	---------

## Discipline: Data Confidentiality and Integrity

---

### Technology Area: Disk Eraser

---

KillDisk 4.1	Twilight
KillDisk Enterprise v5.2	Current

### Technology Area: Encryption Controls

---

Check Point Full Disk Encryption	Current
Check Point Media Encryption	Current
Entrust Entelligence	Current
Microsoft Encrypted File Service (EFS)	Current



# Technology Architecture Product Standards

**Technology Area: Message Digest/Signing**

---

**Discipline: Encryption**

---

**Technology Area: Hash Functions**

---

SHA-1	Current
SHA-256	Current
SHA-384	Current
SHA-512	Current



# Technology Architecture Product Standards

## Domain: Systems Management

### Discipline: Access Management

#### Technology Area: Internet Access

Host on Demand (HOD) +	Twilight
------------------------	----------

#### Technology Area: TP Monitors

CICS	Current
IMS/DC	Current
Roscoe	Current
TSO	Current

### Discipline: Asset and Configuration Management

#### Technology Area: CMDB

BMC Configuration Management	Current
------------------------------	---------

#### Technology Area: Discovery and Inventory

EMC Smarts Application Discovery Manager	Current
Microsoft SCCM	Current
Novell ZENWorks	Obsolete
Novell ZENWorks v10	Emerging

#### Technology Area: Repository for Asset Management

BMC Remedy Asset Management Application	Current
BMC Remedy Asset Management Application 7.1	Current

### Discipline: Change Management

#### Technology Area: Change Management

BMC Remedy Change Management	Current
------------------------------	---------



# Technology Architecture Product Standards

## Discipline: Continuous Service Improvement

**Technology Area: Service Improvement**

**Technology Area: Service Measurement**

**Technology Area: Service Reporting**

## Discipline: Data Storage

**Technology Area: Network Attached Storage (NAS)**

**Technology Area: Storage Area Network (SAN)**

**Technology Area: Storage Management**

CA-1	Current
SAMS/Allocate	Current
SAMS/Vantage	Current
SMS	Current

## Discipline: Event Management

**Technology Area: Job Management**

CA AutoSys	Current
CA11 Mainframe	Current
CA7 Mainframe	Current

**Technology Area: Performance Tuning**

HP OpenView	Current
IBM Netview	Current
Insite Manager	Current
Optivity	Current
The Monitor for IMS (formerly TMON/IMS until 1/15/2004)	Current
TMON/CICS	Current



# Technology Architecture Product Standards

TMON/DB2 3.3	Current
TMON/MVS	Current

## Discipline: Help Desk and Problem Management

### Technology Area: Help Desk/Problem Management

BMC Remedy Action System 6	Current
BMC Remedy SRM	Current

## Discipline: Incident Management

### Technology Area: Incident Management

## Discipline: Middleware Management

### Technology Area: Middleware Management

Jboss Operations Network (JON)	Current
--------------------------------	---------

## Discipline: Operations Management

### Technology Area: Backup/Retrieval

ArcServe	Twilight
FDR	Current
HSM	Current
Veritas NetBackup 5.1	Twilight
Veritas NetBackup 6.1	Current
Veritas NetBackup 6.5	Current
Veritas NetBackup 7.0	Emerging

## Discipline: Release and Deployment Management

### Technology Area: Release and Deployment Management

### Technology Area: Software Distribution



# Technology Architecture Product Standards

Novell ZENWorks	Obsolete
Novell ZENWorks v10	Emerging

## Discipline: Request Fulfillment

**Technology Area: Request Fulfillment**

## Discipline: Service/Business Continuity

**Technology Area: Business Resumption**

**Technology Area: Disaster Recovery**

Paradigm Systems International OpsPlanner	Current
---	---------

## Discipline: Training

**Technology Area: Computer Based Training**

Phoenix	Twilight
---------	----------

**Technology Area: Web Based Training**

Adobe Authorware	Current
------------------	---------



## Enterprise Information Security Policies

**State of Tennessee**  
**Department of Finance and Administration**  
**Office for Information Resources**  
Information Security Program



## Table of Contents

Page

<b>1. EXECUTIVE SUMMARY</b>	<b>1</b>
<b>2. INTRODUCTION</b>	<b>3</b>
Scope (2.1)	4
Authority (2.2)	4
Exceptions (2.3)	5
Review (2.4)	5
Document Format (2.5)	6
Policy Maintenance (2.6)	6
<b>3. GENERAL INFORMATION SECURITY POLICY</b>	<b>7</b>
<b>4. ORGANIZATIONAL SECURITY POLICY</b>	<b>9</b>
Information Security Infrastructure (4.1)	9
Incident Response Policy (4.2)	9
Incident Response Plan (4.3)	10
<b>5. ASSET CLASSIFICATION AND CONTROL POLICY</b>	<b>11</b>
Accountability of Assets (5.1)	11
Data Classification (5.2)	11
Public Data Classification Control (5.2.1)	11
Confidential Data Classification Control (5.2.2)	11
<b>6. PERSONNEL SECURITY POLICY</b>	<b>13</b>
Personnel Background Investigation (6.1)	13
Acceptable Use Policy (6.2)	13
<b>7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY</b>	<b>14</b>
Secure Areas (7.1)	14
Physical Security Perimeter (7.1.1)	14
Equipment Security (7.2)	14
Equipment Placement and Protection (7.2.1)	14
Power Supplies (7.2.2)	14
Cabling Security (7.2.3)	15
General Security Controls (7.3)	15
Clear Screen Policy (7.3.1)	15
<b>8. COMMUNICATIONS AND OPERATIONS MANAGEMENT POLICY</b>	<b>16</b>
Operational Procedures and Responsibilities (8.1)	16
Documentation of Operating Procedures (8.1.1)	16

For Public Release



**Operational Change Control (8.1.2) 16**  
**Segmentation and Layered Security (8.1.3) 16**  
Segregation of Duties (8.1.4) 16  
Separation of Development and Production Facilities (8.1.5) 16  
Production Environment Access Control (8.1.6) 16  
System Planning and Acceptance (8.2) 17  
System Acceptance (8.2.1) 17  
Capacity Planning (8.3) 17  
**Software Control (8.4) 17**  
**Authorized and Licensed Software (8.4.1) 17**  
**Malicious Software Control (8.4.2) 17**  
**Compromised System Policy (8.4.2.1) 17**  
**Patch Management Control (8.4.3) 17**  
**Media Handling and Security (8.4.4) 17**  
Application Control (8.4.5) 17  
**Media Disposal and Reuse (8.5) 18**

## **9. ACCESS CONTROL POLICY 19**

**Access Control Rules (9.1) 19**  
**User Access Management (9.2) 19**  
User Registration and Authorization (9.2.1) 19  
Loss of User Privilege (9.2.1.1) 19  
User Privilege Control (9.2.2) 19  
**User Identification and Authorization (9.2.3) 20**  
**User Account Lockout (9.2.4) 20**  
**User Password Management (9.2.5) 20**  
Review of User Access Rights (9.2.6) 20  
**Network Access Control (9.3) 20**  
User Authentication for Network Connections (9.3.1) 20  
**Segregation in Networks (9.3.2) 20**  
**Enterprise Interconnectivity Requirements (9.3.3) 21**  
Operating System Access Control (9.4) 21  
Session Time Outs (9.4.1) 21  
Password Management System (9.4.2) 21  
Use of Shared Technology Resources (9.4.3) 21  
**Logon Banner (9.4.4) 21**  
**Mobile and Workstation Computing (9.5) 21**  
**Mobile Computing Policy (9.5.1) 21**  
**Workstation Computing Policy (9.5.2) 21**  
Monitoring System Access and Use (9.6) 21  
Event Logging (9.6.1) 21  
Clock Synchronization (9.6.2) 22

## **10. SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY 23**

## **11. COMPLIANCE POLICY 24**

**Compliance with Legal Requirements (11.1) 24**



For Public Release

**Applicable Legislation (11.1.1) 24**

**Data Protection and Privacy (11.1.2) 24**

**Data Breach and Disclosure (11.1.3) 24**

**Internal Compliance Matrix (11.2) 24**

**12. BUSINESS CONTINUITY MANAGEMENT POLICY 25**

**13. VERSION HISTORY 26**

**14. TERMS AND DEFINITIONS 27**

**15. APPENDICES 28** For Public Release



## 1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the availability, integrity and confidentiality of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been developed to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- . All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- . Any computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- . All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

This document applies to all full- and part-time employees of the State of Tennessee and all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency IT professionals and approval by the Chief Information Security Officer (CISO) and executive management team within the Office for Information Resources, Department of Finance and Administration. For Public Release



All information resources and any information system owned by the State of Tennessee shall be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the state government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee as well as the General Information Security Policy of the State of Tennessee. For Public Release



## 1. INTRODUCTION

### **The Information Security Challenge**

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the “just in time” requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes cutting out existing processes which could introduce delays, or bypassing process requirements all together to keep up with the demand of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need and put the information security programs to work. One of the main goals of any successful information security program is to protect the organization’s revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policy is a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 17799 standard framework. The policies are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment. For Public Release



### **Scope (2.1)**

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- . All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) controlled by the State of Tennessee where lawfully permitted.
- . Any computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.
- . All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

All full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms shall adhere to the policies and requirements set forth in this document.

### **Authority (2.2)**

The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Office for Information Resources (OIR) to establish and enforce policy and statewide standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. The Office for Information Resources is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

#### **Reference:**

*Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994*  
*ISC Information Resource Policies, Policy 1.00*  
*ISC Information Resource Policies, Policy 13.00 For Public Release*

**Exceptions (2.3)**

All exceptions to any of the security policies shall be reviewed by the Security Advisory Council (SAC) and approved by the Chief Information Security Officer. The exception request process and form can be found in the appendix of this document.

**Review (2.4)**

Review of this document takes place within the Security Advisory Council sessions and will occur on a semi-annual basis at a minimum. Document review can also be requested by sending a request to the OIR Security Management Team.

The official policy document and supporting documentation will be published on the OIR intranet site located at:

<http://intranet.state.tn.us/finance/oir/security/policy.html> For Public Release

**Document Format (2.5)**

This document generally follows the International Standards Organization (ISO) 17799 standard framework for information technology security management. Each section starts with a high-level policy statement for the domain that is discussed in that section. The high-level policy statement is followed by the objectives of the section. More detailed or specific policy statements follow the objectives. The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise. Finally, the section closes with a description of responsibilities for the Office for Information Resources, agencies and individuals.

**X. Section Name**

*High-level policy statement for section*

**OBJECTIVES:****Policy Name(x.x)**

*Policy statement.*

**Sub-Policy Name(x.x.x)**

*Sub-policy statement.*

**Policy Name(x.x)**

*Policy statement.*

**Policy Maintenance (2.6)**

All policies will be maintained in accordance with the OIR policy process documentation. See the Security Policy Development and Implementation Process located in the appendix of this document. For Public Release



## 1. GENERAL INFORMATION SECURITY POLICY

*All information resources and information systems owned by the State of Tennessee shall be protected from unauthorized disclosure, use, modification or destruction in a manner consistent with their value, sensitivity and criticality to the business and operation of the state government and those it serves. The State of Tennessee shall institute an information security program to define the overall information security policy and direction.*

### **OBJECTIVES:**

- . Ensure that the State of Tennessee's information resources are adequately and appropriately protected against unavailability, unauthorized access, modification, destruction or disclosure as required by the Information Systems Council of the State of Tennessee.
- . Ensure that the State of Tennessee provisions an information security program to uphold the State of Tennessee's information security requirements.
- . Ensure that authorized access to the State of Tennessee's information resources is appropriately provisioned.
- . Prevent disruption of business processes or service delivery caused by information security inadequacies.
- . Ensure that the information security posture of the State of Tennessee is appropriately, efficiently and effectively communicated to the stakeholders of the State of Tennessee.
- . Define and assign responsibilities for protecting information technology resources.

### **RESPONSIBILITIES:**

#### ***OIR***

OIR is responsible for establishing and maintaining a statewide information security policy and security program. OIR will ensure that any information processing system attached to the State of Tennessee's enterprise network and managed by OIR, or on behalf of OIR, is compliant with this policy document. OIR will ensure that this policy document and any subsequent additions, changes or deletions are communicated appropriately to all agencies of State government.

#### ***Agency***

Agencies are responsible for ensuring that any information processing system attached to the State of Tennessee's enterprise network and managed by the agency, or on behalf of the agency, is compliant with this policy document. Agencies are responsible for developing and implementing procedures and operations processes that support the goals and objectives of this policy document. Agencies may develop agency-specific policy documents provided the minimum requirements set forth in this document are met. Agencies are responsible for communicating this policy document throughout the agency. For Public Release

#### ***Users***

Users are responsible for adhering to statewide and agency policies, standards, procedures and guidelines pertaining to information security. For Public Release



## 1. ORGANIZATIONAL SECURITY POLICY

*The State of Tennessee shall maintain an organization within the Office for Information Resources (OIR) that is directly responsible for the direction and strategy of the information security program within the State of Tennessee and for all agencies of Tennessee state government. This group shall be led by the Chief Information Security Officer (CISO) who is ultimately responsible for the direction of the program and for reporting on the State's security posture to the Chief Information Officer (CIO) of the State of Tennessee. Each state agency shall appoint an information security "point of contact" (POC).*

### **OBJECTIVES:**

- . Ensure that the State of Tennessee provisions an information security organization, led by a Chief Information Security Officer, to support the State of Tennessee's information security requirements.
- . Ensure that the information security program can adequately address the requirements set forth by the Information Systems Council.
- . Ensure that the State of Tennessee provisions an information Security Incident Response Team with appropriate resources to exercise the State of Tennessee's information security incident response plan when appropriate.
- . Ensure that agencies designate a knowledgeable information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding information security within the agency.

### **Information Security Infrastructure (4.1)**

*OIR Security Management shall initiate and control an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.*

### **Incident Response Policy (4.2)**

*The State of Tennessee shall establish an information Security Incident Response Team (SIRT). The SIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The SIRT members will be appointed based on their position and capabilities within the organization. Each agency shall designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC shall have responsibility for incident escalations, actions and authority for the administrative oversight of security for the information technology resources under the agency's control. The POC within each agency will*

For Public Release



*participate as a member of the SIRT. The CISO of the State of Tennessee will appoint members from within OIR to participate in the SIRT.*

**Incident Response Plan (4.3)**

*See the appendix of this document.*

**RESPONSIBILITIES:**

***OIR***

OIR is responsible for the establishment of the information security organization as well as the appointment of a Chief Information Security Officer (CISO). The CISO is responsible for the fostering, leadership and communication of the State of Tennessee's enterprise security program. The CISO shall establish a Security Advisory Council (SAC). As Chair of the Security Advisory Council (SAC), the CISO will ensure that the proper representatives are appointed to the SAC and will lead the SAC's efforts to develop, implement and maintain an information security program for the State of Tennessee. The CISO will chair the SIRT and ensure that it will be appropriately staffed and provisioned, organized, maintained, and will include a representative from each agency. The CISO will also ensure that an information security response plan is developed, maintained, and distributed to all agencies.

***Agency***

Agencies are responsible for appointing an information security POC. In accordance with ISC policies, the agency POC will have the responsibility and authority for the administrative oversight of security for information resources under the agency's control. The POC shall be available to work with the SIRT and knowledgeable of the information incident response plan. Further, agencies will ensure that the agency POC participates in the "Tennessee Agency Security Advisory Group" chaired by the CISO.

***Users***

Users are responsible for reporting suspected or known security violations to the agency's POC and for following instructions pertaining to specific incidents as provided by SIRT members. For Public Release



## 1. ASSET CLASSIFICATION AND CONTROL POLICY

*All information resource assets owned by the State of Tennessee shall be classified in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification or destruction. Classified assets shall be protected in a manner consistent with their value, sensitivity and criticality to the business and operation of the state government and those it serves or as specified by any superseding State or Federal law or regulation.*

### **Accountability of Assets (5.1)**

*All information resource assets owned by the State of Tennessee shall be accounted for and have a designated custodian. Custodians shall be identified for all information resource assets by each State agency, and the responsibility for the maintenance of appropriate controls, or stewardship, shall be assigned for the assets under the agency's control. Accountability shall remain with the designated custodian of the asset.*

### **Data Classification (5.2)**

*Data stored or transferred by information resource assets owned by the State of Tennessee shall be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable State and/or Federal law and regulations to indicate the need, priorities and degree of protection it will receive. At a minimum data shall be classified as public or confidential.*

#### **Public Data Classification Control (5.2.1)**

*Data classified as public shall be protected from unauthorized modification or destruction.*

#### **Confidential Data Classification Control (5.2.2)**

*Data classified as confidential shall be protected from unauthorized disclosure, use, modification or destruction.*

## **RESPONSIBILITIES:**

### **OIR**

OIR is responsible for the development and maintenance of the statewide information resources asset classification requirements. OIR shall identify asset custodians for the information resources under their direct control. OIR asset custodians shall classify the assets under their control at the time the assets are assigned or created. Asset classification and maintenance can be delegated to an asset steward supervised by the asset custodian. For Public Release

**Agency**

Agencies are responsible for identifying asset custodians for the resources under their direct control. Agency asset custodians shall classify the assets under their direct control at the time the assets are assigned or created. Asset classification and maintenance can be delegated to an asset steward supervised by the asset custodian.

**Users**

Users shall responsibly work with the assets they are assigned and due care shall be taken to protect any mobile computing asset from theft or destruction. Users shall not provide access to information resource assets without obtaining authorization from the asset custodian. For Public Release

**1. PERSONNEL SECURITY POLICY****Personnel Background Investigation (6.1)**

Under Development

**Acceptable Use Policy (6.2)**

See the appendix of this document. For Public Release

**1. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY**

*Physical access to the State of Tennessee's information resource assets and infrastructure will be restricted to individuals who require that access to perform their job function.*

**OBJECTIVES:**

- . To prevent unauthorized access, damage or interference to State of Tennessee premises and information.
- . To prevent loss, damage or compromise of processing equipment or network components.

**Secure Areas (7.1)**

*Critical/sensitive business information processing facilities shall be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls that protect them from unauthorized access, damage and/or interference.*

**Physical Security Perimeter (7.1.1)**

*All critical/sensitive enterprise processing facilities shall have multiple layers of physical security. Each layer shall be independent and separate of the preceding and/or following layer(s).*

*All other processing facilities shall have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.*

**Equipment Security (7.2)**

*Processing equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and to reduce the opportunities for unauthorized access.*

**Equipment Placement and Protection (7.2.1)**

*Equipment shall be located in secured areas. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter shall be locked in a secured cabinet with access controlled by the State of Tennessee. Secured cabinets or facilities shall support*



*further segregation within the State of Tennessee's Information Technology (IT) organization based on role and responsibility.*

**Power Supplies (7.2.2)**

*Infrastructure and related computing equipment shall be protected from power failures and other electrical anomalies.* For Public Release

**Cabling Security (7.2.3)**

*Power and telecommunications cabling carrying data or supporting information services shall be protected from unauthorized interception or damage.*

**General Security Controls (7.3)**

*Information shall be protected from disclosure to, modification or theft by unauthorized persons.*

**Clear Screen Policy (7.3.1)**

*All endpoints that provide access to Information Processing Systems shall be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system shall automatically be implemented if the system has been left unattended.*

*All computing platforms with attached displays shall be oriented away from direct line of sight from unauthorized viewers.*

**RESPONSIBILITIES****OIR**

OIR is responsible for developing requirements and guidelines for physical access to enterprise information resource assets and infrastructure. OIR will ensure that appropriate protective mechanisms are installed to restrict access to the enterprise information resource assets and infrastructure, in coordination with appropriate departments. Further, OIR will ensure physical access to enterprise assets is monitored, and unauthorized access is reported to management or the proper authorities.

**Agency**

Agencies are responsible for implementing practices and procedures and installing protective mechanisms to ensure local information assets are protected from unauthorized access. Agencies are also responsible for ensuring that physical access to agency hosted assets is monitored and that unauthorized access is reported to management or the proper authorities.

**Users**

Users should report any suspicious activity or persons to management or the proper authorities. Users should also refrain from behaviors that could compromise the physical protection of information technology resources such as willful assistance without proper identification, tailgating through doors or sharing facility access keys or codes. For Public Release



## 1. COMMUNICATIONS AND OPERATIONS MANAGEMENT POLICY

*All agencies of the State of Tennessee shall document and maintain standard security operating procedures and configurations for their respective operating environments.*

### **OBJECTIVES:**

- . Reduce the risk of liability for the unauthorized usage of unlicensed software and minimize the threat of exposure due to software weaknesses and/or configurations.
- . Prevent the automated propagation of malicious code and contamination of sterile environments attached to the enterprise network.
- . Ensure that media resources containing sensitive data are sanitized before transferal or reuse and that they are destroyed when decommissioned and not selected for reuse or transfer.
- . Protect critical state information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction.

### **Operational Procedures and Responsibilities (8.1)**

*The operating procedures identified by the security policy shall be documented and maintained by the appropriate process owners.*

#### **Documentation of Operating Procedures (8.1.1)**

*Operating procedures relating to security shall be treated as formal documents and changes shall be authorized by management.*

#### **Operational Change Control (8.1.2)**

*Changes to information processing facilities and systems shall be controlled and monitored for security compliance. Formal management responsibilities and procedures shall exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of the State of Tennessee's operational environment.*

*All written documentation generated by the change control policies shall be retained as evidence of compliance.*

#### **Segmentation and Layered Security (8.1.3)**

*The State of Tennessee's operational environment shall support segmentation and layered security technologies and configurations based on role, risk, sensitivity and access control rules.*

#### **Segregation of Duties (8.1.4)**

#### **Separation of Development and Production Facilities (8.1.5)**

#### **Production Environment Access Control (8.1.6)**

*Under Development For Public Release*



## **System Planning and Acceptance (8.2)**

### **System Acceptance (8.2.1)**

*Under Development*

### **Capacity Planning (8.3)**

*Under Development*

### **Software Control (8.4)**

*All software installed within the State's operational environment shall support security mechanisms that provide data integrity, confidentiality and availability. Software shall support security event monitoring and audit ability.*

#### **Authorized and Licensed Software (8.4.1)**

*Only licensed software procured through State of Tennessee contracts or software acquired with Office for Information Resources (OIR) involvement in the procurement process shall be installed in the State's environment. Software that does not require a purchase (i.e. General Public License, FreeWare, ShareWare) shall be approved as a State standard software product through the State's architecture standards approval process.*

#### **Malicious Software Control (8.4.2)**

*All computing platforms that are attached to the State's enterprise technology infrastructure shall be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses and/or logic bombs.*

##### **Compromised System Policy (8.4.2.1)**

*Any system found infected with "Rootkit" malicious software is considered fully compromised. Fully compromised systems shall be removed from the operational environment. OIR Security Management reserves the right to seize any compromised system for forensic analysis.*

#### **Patch Management Control (8.4.3)**

*All applications and processing devices that are attached to the State's enterprise technology infrastructure shall be kept up to date with security related patches made available by the software or hardware vendor.*

#### **Media Handling and Security (8.4.4)**

*Software licensed to the State of Tennessee shall be installed only on systems or devices covered by the license agreement.*

#### **Application Control (8.4.5)**

*Under Development For Public Release*

**Media Disposal and Reuse (8.5)**

*All data storage devices (media) subject to transfer or reuse must be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding State or Federal requirements. Media assets that are not subject to transfer or reuse must be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding State or Federal requirements.*

**RESPONSIBILITIES:*****OIR***

OIR is responsible for maintaining network infrastructure and enterprise component software and operating system configurations with the latest release of security related updates compatible with the State's enterprise environment and will provide a means by which authentic, tested and approved security related software updates can be deployed and implemented by agencies across the enterprise. OIR will deploy and monitor security control devices to facilitate a means by which all processing devices attached to the enterprise network environment can be protected from intentional or unintentional exposure to malicious software. OIR will establish, maintain, and follow procedures to prevent the propagation of malicious code and/or system abuse. OIR will develop and maintain supporting guidelines and documentation and will ensure that contracts for standard software products and media destruction services are maintained. Finally, OIR will work with vendors/contractors (engaged through OIR) and who are responsible for non-state managed devices to ensure they understand and comply with these responsibilities.

***Agency***

Agencies will establish agency policy and procedures for media disposal or reuse, including personally and/or contractor owned devices, and will ensure that any agency media disposal and reuse procedure complies with superseding State or Federal sanitizing requirements that may be specific for the agency. Agencies systems attached to the State of Tennessee's enterprise network will participate in enterprise patch management and malicious software control programs. Agencies will be responsible for testing patches prior to release in the agency's environment. Agencies will also ensure that all systems not able to participate in an automatic security related update process are kept up to date through an additional manual process. This process, along with the participating systems, must be documented and made available for periodic audit by the OIR Security Management Team. Agencies will utilize software products that have been approved as standard for the State of Tennessee. Finally, agencies will ensure vendors/contractors (engaged through the agency) who are responsible for non-state-managed devices understand and comply with these responsibilities.

***Users***

Users are responsible for ensuring that devices assigned to them retain the ability to participate in automatic security software update environments (i.e. Disabling automatic enterprise configurations is prohibited). Users are to only utilize software products that have been approved as standard for the State of Tennessee, and they are to abstain from downloading unauthorized software or installing personally owned software For Public Release.



## 1. ACCESS CONTROL POLICY

*Access to the State of Tennessee's information resources shall be granted consistent with the concept of least privilege. All information processing systems owned by the State of Tennessee shall have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use. All information processing systems shall have the capability to interact with the statewide access control environment. Access to any State of Tennessee information processing system is generally forbidden unless explicitly permitted.*

### **OBJECTIVES:**

- . Ensure that authorized access to the State of Tennessee's information resources is appropriately provisioned.
- . Ensure that unauthorized access to information resources is appropriately prevented.
- . Minimize information technology risks through the use of access control methodologies and techniques.
- . Ensure that a means to segment and control enterprise network traffic is implemented.
- . Ensure that all interconnectivity between the State of Tennessee's enterprise network and any other network is provisioned securely.

### **Access Control Rules (9.1)**

*Access control rules and requirements to access the State of Tennessee's information resources shall be developed, documented and maintained by their respective resource owners. All agency specific-access control rules and requirements must be made available for audit by the Office for Information Resources (OIR) Security Management Team and in compliance with the State of Tennessee enterprise security policies. All enterprise access control rules and requirements must be approved by the OIR Security Management Team.*

### **User Access Management (9.2)**

*All State of Tennessee agencies shall develop, document and maintain user access and account management procedures. These procedures shall include, but are not limited to, new account provisioning, account transfer and/or job profile changes and account termination and/or de-provisioning.*

#### **User Registration and Authorization (9.2.1)**

##### **Loss of User Privilege (9.2.1.1)**

##### **User Privilege Control (9.2.2)**

*Under Development For Public Release*

**User Identification and Authorization (9.2.3)**

*At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.*

**User Account Lockout (9.2.4)**

*Limits shall be set for the number of unsuccessful logins that can be attempted for a UserID.*

**User Password Management (9.2.5)**

*Passwords assigned to users must be created and managed to protect against unauthorized discovery or usage and must meet the minimum password requirements.*

**Review of User Access Rights (9.2.6)**

*Under Development*

**Network Access Control (9.3)**

*The State of Tennessee's enterprise network shall be designed to provide the ability to segregate and control traffic between systems, connected devices and third party environments based on role, risk and sensitivity. The enterprise network will allow for specific services at all seven layers of the Open Systems Interconnection (OSI) model to be made available or filtered, depending on legitimate business need. All access and connectivity to the State of Tennessee's enterprise network must comply with the State of Tennessee's security requirements for enterprise network interconnectivity. All access and connectivity to the State of Tennessee's enterprise network shall be granted consistent with the concept of least privilege. Access and connectivity to the State of Tennessee's enterprise network is generally forbidden unless explicitly permitted.*

**User Authentication for Network Connections (9.3.1)**

*Under Development*

**Segregation in Networks (9.3.2)**

*All enterprise network architectures operated by, or on behalf of, the State of Tennessee shall be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones shall be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the OIR Security Management Team. For Public Release*

**Enterprise Interconnectivity Requirements (9.3.3)**

*All systems attached to the State of Tennessee's enterprise network shall comply with the security requirements for enterprise interconnectivity documentation.*

**Operating System Access Control (9.4)****Session Time Outs (9.4.1)****Password Management System (9.4.2)****Use of Shared Technology Resources (9.4.3)**

*Under Development*

**Logon Banner (9.4.4)**

*All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user logs in.*

**Mobile and Workstation Computing (9.5)**

*All mobile and workstation computing platforms, including but not limited to desktops, laptops, hand-held devices, and portable storage media, shall be protected from unauthorized use, modification or destruction. Mobile and workstation computing platform capabilities shall be granted to individuals or entities that require such access and facilities to perform their specific job related duties. Confidential data assets shall not be stored on mobile and/or workstation computing platforms unless absolutely necessary.*

**Mobile Computing Policy (9.5.1)**

*Mobile computing platforms shall be physically protected against theft when left unattended. Mobile computing platforms shall not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a mobile computing platform must have approval from the asset custodian for such storage. Confidential data assets which have been authorized for mobile use must be encrypted while stored on mobile computing platforms.*

**Workstation Computing Policy (9.5.2)**

*Workstation computing platforms shall be physically protected against theft when left unattended. Workstation computing platforms shall not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a workstation computing platform must have approval from the asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation must be encrypted while stored on the workstation computing platform.*

**Monitoring System Access and Use (9.6)****Event Logging (9.6.1) For Public Release**



## **Clock Synchronization (9.6.2)**

*Under Development*

### **RESPONSIBILITIES:**

#### **OIR**

will ensure that all enterprise networks are provisioned and segmented with the appropriate levels of security in regards to role, risk and sensitivity. They will also develop, implement and maintain guidelines for password management and maintenance. OIR will ensure that all third parties are aware of and compliant with the State of Tennessee's Third Party Connectivity Agreement prior to the establishment of the interconnection. OIR is responsible for the management and processing of granting or rejecting third party interconnectivity requests. OIR shall ensure that due diligence and care is taken to fulfill any protection requirements of the mobile computing platforms for which OIR is responsible.

#### **Agency**

Agencies are responsible for implementing a process for identifying and documenting legitimate "need" for users to have access to the State of Tennessee's information resources. This process will include review and revalidation of existing users. Agencies will ensure that all requirements of a third party network connection to the State of Tennessee's enterprise network are presented to the OIR Security Management Team for review, approval or rejection prior to implementing the connection. Agencies shall ensure that due diligence and care is taken to fulfill any protection requirements of the mobile computing platforms for which each agency is responsible.

#### **Users**

Individual users are uniquely identified by their respective access credentials and are responsible for maintaining the confidentiality of those credentials. Users should refrain from using authentication credentials intended for the protection of State of Tennessee assets on personal computing platforms or non-State related websites. For Public Release

## 1. **SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY** **Systems Development and Maintenance Control Policy 10.0**

*Under Development*

For Public Release

## 1. **COMPLIANCE POLICY**

*All State of Tennessee agencies must be compliant with this security policy document*

### **Compliance with Legal Requirements (11.1)**

*All State of Tennessee agencies must be compliant with any State or Federal regulatory requirements which supersede this policy document.*

#### **Applicable Legislation (11.1.1)**

*All State of Tennessee agencies must be compliant with any legislation enacted by the State of Tennessee in regards to the management of information resources on behalf of the State.*

#### **Data Protection and Privacy (11.1.2)**

*All State of Tennessee agency data custodians must ensure that all "Personal Information" data assets, as defined by applicable State and/or Federal law and regulations, are protected from unauthorized use, modification or disclosure.*

**Data Breach and Disclosure (11.1.3)**

*Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties shall provide notice of the disclosure in accordance with TCA 47-18-2107(3)(A).*

**Internal Compliance Matrix (11.2)**

See the Appendix of this document for the policy compliance matrix, which indicates the dates by which all agencies must be compliant with the relative policy components. Those agencies that cannot meet the compliance deadline must file for an exception using the security policy exception process. For Public Release

**1. BUSINESS CONTINUITY MANAGEMENT POLICY**

While Business Continuity Management is included in the International Standards Organization (ISO) 17799 standards, it is outside the scope of the security organization within OIR. Agencies are expected to collaborate with the State's administrative services agencies to ensure their ability to recover from any disaster and to maintain business operations. For Public Release



## 1. VERSION HISTORY

Version 1.0 – May 10, 2006	<i>Initial draft review to agencies and SAC.</i>
Version 1.1 – June 27, 2006	<i>Fixed errors before official release.</i>
Version 1.2 – July 12, 2006	<i>Added policies 5.0, 5.1, 5.3, 5.3.1, 9.5, 9.5.1, 11.1, 11.1.1, 11.1.2, 11.1.3 for SAC review.</i>
Version 1.3 – July 26, 2006	<i>Made modifications as a result of the SAC and legal commentary to sections 1,2,5,9 and 11.</i>
Version 1.3 – August 15, 2006	<i>Minor adjustments to new policies introduced in v1.2 and v1.3, fixed spelling errors.</i>
Version 1.3 – September 14, 2006	<i>Version 1.3 approved for publication.</i>
Version 1.4 – August 8, 2007	<i>Minor wording changes throughout. Major wording changes to 9.5.</i>
Version 1.5 – January 8, 2008	<i>Minor wording changes to 9.5. Added policy 9.5.2.</i>
Version 1.6 – April 4, 2008	<i>Minor wording changes to 9.5.2.</i>