



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 2
 to
 Contract Number 190000000477

CONTRACTOR	ACCENTURE
	One Financial Plaza, 755 Main Street
	Hartford, CT 06103
	Lisa Cawley
	589-248-1187
	kathleen.cawley@accenture.com
	CV0062320

STATE	Program Manager	Jeff Anderson	MDOC
		517-335-1251	
		AndersonJ30@michigan.gov	
	Contract Administrator	Douglas Glaser	DTMB
		517-898-3982	
		glaserd@michigan.gov	

CONTRACT SUMMARY

ORGANIZATIONAL CHANGE MANAGEMENT (OCM) FOR Offender Management System (COMS) - MDOC

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE PTIONS	EXPIRATION DATE BEFORE
April 5, 2019	December 31, 2020	1 - 1 Year	December 31, 2020
PAYMENT TERMS		DELIVERY TIMEFRAME	
NET 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$2,200,000.43	\$0.00	\$2,200,000.43		

DESCRIPTION

Effective 4/3/2020, the following amendment is hereby incorporated into the contract, per attached update.

Please note the Standard Contract Terms section 3 has been changed to Doug Glaser, glaserd@michigan.gov, 517-898-3982.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.



Below is the listing of **Schedule A - Statement of Work Contract Activities (Dated April 18, 2019)** language changes, revisions, and additions are highlighted and bold, deleted phrases or words are struck through. Schedule A was updated with Change Notice #1 and the changes below are updates to that newer Statement of Work:

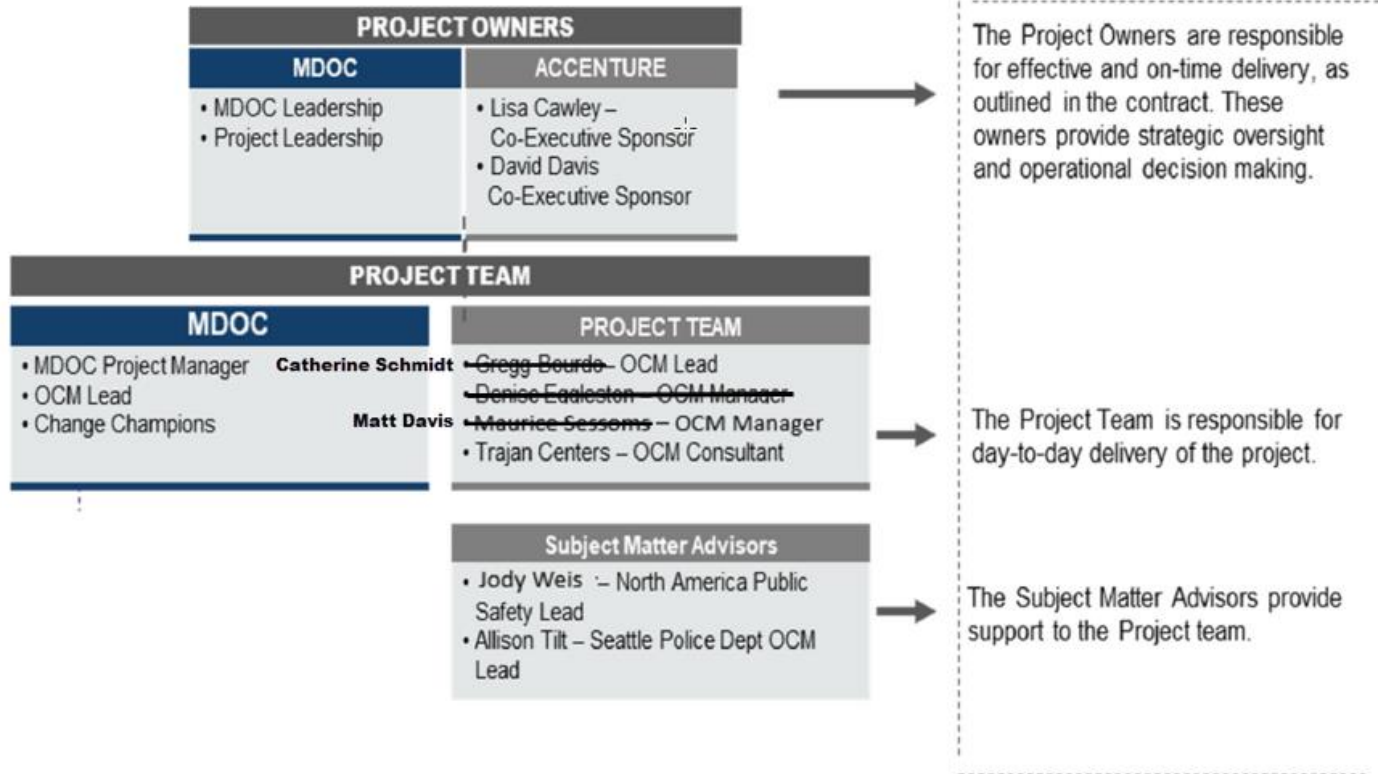
<p>Change Notice #1 Page 2 of 9</p> <p>2. Contract Activities</p> <p>Understanding Change Impacts</p>	<p>The second bullet has been removed to reflect the change:</p> <p>Understand Change Impacts</p> <p>Contractor will identify the impact of the COMS implementation on MDOC people, processes, and technology to inform change activities and training. Key Contract Activities include:</p> <ul style="list-style-type: none"> • Completing a stakeholder impact assessment by attending conference room pilot sessions and/or design sessions for the new COMS system and working collaboratively with the system vendor. ; or, • Facilitating Contractor led sessions to identify the location of the biggest impacts on the day to day work of COMS users, enable MDOC to proactively identify business process changes, and recommend a course of action to prepare the workforce through communications and readiness activities.
--	---

<p>Change Notice #1 Page 3 of 9</p> <p>3. OCM Project Schedule</p>	<p>The graphic below updates and replaces the original graphic, which removes the Business Process Impact Tracker</p> <table border="1"> <thead> <tr> <th>Deliverables</th> <th>Apr-2019</th> <th>May-2019</th> <th>Jun-2019</th> <th>Jul-2019</th> <th>Aug-2019</th> <th>Sep-2019</th> <th>Oct-2019</th> <th>Nov-2019</th> <th>Dec-2019</th> <th>Jan-2020</th> <th>Feb-2020</th> <th>Mar-2020</th> <th>Apr-2020</th> <th>May-2020</th> <th>Jun-2020</th> <th>Jul-2020</th> </tr> </thead> <tbody> <tr> <td>All Milestones (All)</td> <td></td> <td></td> <td>All</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Food Service (FS)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Healthcare (HC)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Trust (TR)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Parole Board/Field Ops (FO/PB)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Meal Track (MT)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Change Management Plan</td> <td></td> <td></td> <td>All</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Knowledge Transfer Plan</td> <td></td> <td></td> <td>All</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Change Network Document</td> <td></td> <td></td> <td>All</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Communications Plan</td> <td></td> <td></td> <td>All</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Readiness Survey Results (TGPS tool)</td> <td></td> <td></td> <td>X</td> <td>All</td> <td></td> <td>X</td> <td>FS</td> <td></td> <td></td> <td>X</td> <td>HC</td> <td></td> <td></td> <td>X, X</td> <td>TR, FO/PB, MT</td> <td></td> </tr> <tr> <td>Knowledge Transfer Scorecard</td> <td></td> <td></td> <td></td> <td></td> <td>FS</td> <td></td> <td></td> <td></td> <td>HC</td> <td></td> <td></td> <td></td> <td></td> <td>TR</td> <td>FO/PB, MT</td> <td></td> </tr> <tr> <td>Customized Stakeholder Action Plans</td> <td></td> <td></td> <td></td> <td>FS</td> <td></td> <td></td> <td></td> <td>HC</td> <td></td> <td></td> <td></td> <td>TR</td> <td></td> <td>FO/PB</td> <td>MT</td> <td></td> </tr> <tr> <td>Facility Readiness Checklists & Dashboard</td> <td></td> <td></td> <td></td> <td></td> <td>FS</td> <td></td> <td></td> <td></td> <td>HC</td> <td></td> <td></td> <td></td> <td></td> <td>TR</td> <td>FO/PB</td> <td></td> </tr> <tr> <td>Communications Material Report</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>FS</td> <td></td> <td></td> <td></td> <td>HC</td> <td></td> <td></td> <td></td> <td></td> <td>TR</td> <td></td> </tr> </tbody> </table>	Deliverables	Apr-2019	May-2019	Jun-2019	Jul-2019	Aug-2019	Sep-2019	Oct-2019	Nov-2019	Dec-2019	Jan-2020	Feb-2020	Mar-2020	Apr-2020	May-2020	Jun-2020	Jul-2020	All Milestones (All)			All														Food Service (FS)																	Healthcare (HC)																	Trust (TR)																	Parole Board/Field Ops (FO/PB)																	Meal Track (MT)																	Change Management Plan			All														Knowledge Transfer Plan			All														Change Network Document			All														Communications Plan			All														Readiness Survey Results (TGPS tool)			X	All		X	FS			X	HC			X, X	TR, FO/PB, MT		Knowledge Transfer Scorecard					FS				HC					TR	FO/PB, MT		Customized Stakeholder Action Plans				FS				HC				TR		FO/PB	MT		Facility Readiness Checklists & Dashboard					FS				HC					TR	FO/PB		Communications Material Report						FS				HC					TR	
Deliverables	Apr-2019	May-2019	Jun-2019	Jul-2019	Aug-2019	Sep-2019	Oct-2019	Nov-2019	Dec-2019	Jan-2020	Feb-2020	Mar-2020	Apr-2020	May-2020	Jun-2020	Jul-2020																																																																																																																																																																																																																																																																	
All Milestones (All)			All																																																																																																																																																																																																																																																																														
Food Service (FS)																																																																																																																																																																																																																																																																																	
Healthcare (HC)																																																																																																																																																																																																																																																																																	
Trust (TR)																																																																																																																																																																																																																																																																																	
Parole Board/Field Ops (FO/PB)																																																																																																																																																																																																																																																																																	
Meal Track (MT)																																																																																																																																																																																																																																																																																	
Change Management Plan			All																																																																																																																																																																																																																																																																														
Knowledge Transfer Plan			All																																																																																																																																																																																																																																																																														
Change Network Document			All																																																																																																																																																																																																																																																																														
Communications Plan			All																																																																																																																																																																																																																																																																														
Readiness Survey Results (TGPS tool)			X	All		X	FS			X	HC			X, X	TR, FO/PB, MT																																																																																																																																																																																																																																																																		
Knowledge Transfer Scorecard					FS				HC					TR	FO/PB, MT																																																																																																																																																																																																																																																																		
Customized Stakeholder Action Plans				FS				HC				TR		FO/PB	MT																																																																																																																																																																																																																																																																		
Facility Readiness Checklists & Dashboard					FS				HC					TR	FO/PB																																																																																																																																																																																																																																																																		
Communications Material Report						FS				HC					TR																																																																																																																																																																																																																																																																		

<p>Change Notice #1 Page 5 of 9</p> <p>4. Deliverables</p> <p>Understand Change Impacts</p> <p>Business Process Impact Tracker</p>	<p>In the table below, the following rows will be deleted as shown.</p> <table border="1"> <thead> <tr> <th>Deliverables</th> <th>Description</th> <th>Deliverable Date</th> </tr> </thead> <tbody> <tr> <td>Understand Change Impacts</td> <td></td> <td></td> </tr> <tr> <td>Business Process Impact Tracker</td> <td>The Business Process Impact Tracker is an Excel document that documents where the biggest impacts will be on day to day work of the users, so that they can be emphasized in both communications and training.</td> <td>07/2019; 11/2019; 03/2020; 05/2020; 06/2020;</td> </tr> </tbody> </table>	Deliverables	Description	Deliverable Date	Understand Change Impacts			Business Process Impact Tracker	The Business Process Impact Tracker is an Excel document that documents where the biggest impacts will be on day to day work of the users, so that they can be emphasized in both communications and training.	07/2019; 11/2019; 03/2020; 05/2020; 06/2020;
Deliverables	Description	Deliverable Date								
Understand Change Impacts										
Business Process Impact Tracker	The Business Process Impact Tracker is an Excel document that documents where the biggest impacts will be on day to day work of the users, so that they can be emphasized in both communications and training.	07/2019; 11/2019; 03/2020; 05/2020; 06/2020;								



<p>Change Notice #1 Page 5 of 9</p> <p>4. Deliverables</p> <p>Communicate for Awareness and Understanding</p> <p>Communications Plan</p>	<p>In the table, the fourth bullet point has been changed from 2-3 per month to 5-6 per month and the Deliverable Date from 6/2019 to 6/2020:</p> <ul style="list-style-type: none"> The communications materials are Word document(s) developed and delivered digitally approximately 2-3 5-6 per month that utilize existing MDOC communication channels (i.e. Corrections Connections newsletter, podcast, etc.) and are focused on the highest impacts to MDOC's staff. Such materials also include the development of analog options such as posters, banners, pocket guides. 																				
<p>Change Notice #1 Page 6 of 9</p> <p>7. Project Team</p>	<p>The following text has been changed to read:</p> <p>Contract Activities will be led by Contractor Senior Manager, Gregg Bourdo Catherine Schmidt, supported by the following Contractor resources:</p> <p>The table has been updated to replace Engagement Lead Gregg Bourdo with Catherine Schmidt (Start Date: 9/1/2019 End Date: 6/12/2020)</p> <p>In the table, the OCM Manager Maurice Sessoms has been replaced with Matt Davis (Start Date: 2/29/2020 End Date: 6/12/2020)</p> <p>In the table, an End Date of 12/31/2019 for Denise Eggleston was added.</p> <table border="1" data-bbox="402 1066 1518 1591"> <thead> <tr> <th>Role</th> <th>Name</th> <th>Start Date</th> <th>End Date</th> </tr> </thead> <tbody> <tr> <td>Engagement Lead</td> <td>Gregg Bourdo Catherine Schmidt</td> <td>4/15/2019 9/1/2019</td> <td>6/12/2020</td> </tr> <tr> <td>OCM Manager</td> <td>Denise Eggleston</td> <td>4/15/2019</td> <td>6/12/2020 12/31/2019</td> </tr> <tr> <td>OCM Manager</td> <td>Maurice Sessoms Matt Davis</td> <td>4/15/2019 2/29/2020</td> <td>6/12/2020</td> </tr> <tr> <td>OCM Analyst</td> <td>Trajan Centers</td> <td>4/15/2019</td> <td>6/12/2020</td> </tr> </tbody> </table>	Role	Name	Start Date	End Date	Engagement Lead	Gregg Bourdo Catherine Schmidt	4/15/2019 9/1/2019	6/12/2020	OCM Manager	Denise Eggleston	4/15/2019	6/12/2020 12/31/2019	OCM Manager	Maurice Sessoms Matt Davis	4/15/2019 2/29/2020	6/12/2020	OCM Analyst	Trajan Centers	4/15/2019	6/12/2020
Role	Name	Start Date	End Date																		
Engagement Lead	Gregg Bourdo Catherine Schmidt	4/15/2019 9/1/2019	6/12/2020																		
OCM Manager	Denise Eggleston	4/15/2019	6/12/2020 12/31/2019																		
OCM Manager	Maurice Sessoms Matt Davis	4/15/2019 2/29/2020	6/12/2020																		
OCM Analyst	Trajan Centers	4/15/2019	6/12/2020																		
<p>Change Notice #1 Page 9 of 9</p> <p>9. Personnel</p>	<p>The graphic below updates and replaces the original graphic as shown:</p>																				



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
 P.O. BOX 30026 LANSING, MICHIGAN 48909



CONTRACT CHANGE NOTICE

Change Notice Number **1**
 to
 Contract Number **19000000477**

CONTRACTOR	ACCENTURE
	One Financial Plaza, 755 Main Street
	Hartford, CT 06103
	Lisa Cawley
	589-248-1187
	kathleen.cawley@accenture.com
	CV0062320

STATE	Program Manager	Jeff Anderson	MDOC
		517-335-1251	
		AndersonJ30@michigan.gov	
	Contract Administrator	Steve Rigg	DTMB
		517-249-0454	
		riggs@michigan.gov	

CONTRACT SUMMARY			
Organizational Change Management (OCM) for the Offender Management System (COMS) - MDOC			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
April 5, 2019	December 31, 2020	1 - 1 Year	December 31, 2020
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
DESCRIPTION OF CHANGE NOTICE			
OPTION	LENGTH OF OPTION	EXTENSION	REVISD EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>	December 31, 2020
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$2,200,000.43	\$0.00	\$2,200,000.43	
DESCRIPTION			
Effective April 18, 2019, the attached Statement of Work represents an amendment to contract 190000000477. All other terms, conditions, specification and pricing remain the same. Per Agency and Contractor approval, and DTMB Central Procurement Services approval.			

STATE OF MICHIGAN

Contract No. 190000000477
MDOC Change Management for COMS Application

SCHEDULE A STATEMENT OF WORK (SOW) CONTRACT ACTIVITIES (Dated April 18, 2019)

The Contract Activities provided by Contractor as further defined below will focus on organizational change management (OCM) with respect to MDOC staff who will use this new system to drive integration. The Project will involve planning activities to create a continuous cycle of discovery, alignment, engagement and communication with MDOC leadership and impacted MDOC employees for a Project duration as described below. The Project will:

- a) Develop a change strategy that outlines the key activities that will be completed during the Project.
- b) Coach COMS program leaders to lead the organization through the high degree of change the COMS implementation will bring.
- c) Prepare impacted stakeholders for changes, as well as identify and address their areas of most concern.
- d) Develop a change network with representatives leading the change locally to encourage accountability and ownership.
- e) Assess potential impacts and resistance, inform training, and prioritize efforts.
- f) Co-create a communications plan and initial messaging that will inform, engage, alert, and explain changes to impacted stakeholders in a timely manner.

1. Term

The Contract Activities will be performed by Contractor commencing April 15, 2019 ("Effective Date"), and are to be completed on June 12, 2020, unless this SOW is otherwise terminated or extended in accordance with the Contract.

2. Contract Activities

The Contract Activities that will be provided in support of the Project are as follows:

Empower Project to Lead

Contractor will develop a Change Management Strategy with the assistance of MDOC leadership.

Key Contract Activities include:

- Conduct one workshop with MDOC leadership to confirm the vision and benefits of the COMS project for messaging and communications.
- Create a change management strategy which outlines OCM activities for the COMS project implementation.
- Incorporate OCM into the existing COMS governance structure such that OCM becomes an integral part of overall Project leadership.

Engage Key Stakeholders

Contractor will complete stakeholder analyses, using Contractor's Transformation Global Positioning System (GPS) analytic asset and capability in providing the Contract Activities, to enable customized change activities and engagement, and alignment on readiness, messaging

and actions needed for each stakeholder group. Outputs from Contractor's proprietary Transformation GPS will enable MDOC to focus on aligning culture, behaviors, and ways of working in support of the COMS implementation by using data from MDOC employees for the duration of the OCM project. MDOC stakeholder groups will be placed on a 3-D performance map, via pattern-mapping to Contractor's database of over 650 change journeys and the use of predictive analytics to enable the team to take an evidence-based approach to drive transformation.

Key Contract Activities include:

- Identifying and segmenting all key stakeholder groups through qualitative and quantitative methods.
- Understanding stakeholders' readiness for change at each key milestone (5 cycles).
- Aligning and adjusting change management activities to stakeholder readiness as information is analyzed in the Transformation GPS analytic asset and capability.

Mobilize Change Network

Contractor will institute a change network comprised of a core set of MDOC change champions, representing different parts of the MDOC organization to leverage peer-to-peer communication, create a two-way communication channel, and build change management skills within MDOC personnel.

Key Contract Activities include:

- Establishing a dedicated peer-to-peer group of stakeholders who can advocate, communicate, and support changes, or "change champions."
- Training MDOC change champions in their new roles.
- Creating a continuous feedback mechanism that enables leaders to be proactive in addressing stakeholder concerns.

Understand Change Impacts

Contractor will identify the impact of the COMS implementation on MDOC people, processes, and technology to inform change activities and training.

Key Contract Activities include:

- Completing a stakeholder impact assessment by attending conference room pilot sessions and/or design sessions for the new COMS system and working collaboratively with the system vendor; or,
- Facilitating Contractor-led sessions to identify the location of the biggest impacts on the day-to-day work of COMS users, enable MDOC to proactively identify business process changes, and recommend a course of action to prepare the workforce through communications and readiness activities.

Communicate for Awareness and Understanding

Contractor will establish and rollout a formal communication strategy to keep stakeholders up-to-date on the COMS project – including what is changing and what is needed from the stakeholders.

Key Contract Activities include:

- Creating and enabling the use of a multi-channel approach aligned to stakeholder readiness and change impact areas.
- Utilizing existing MDOC communication channels, (i.e. Corrections Connections newsletter, podcast, etc.) (and creating new communication channels) that are intended to increase awareness and understanding of the COMS project and the resulting process changes.
- Provide consistent and targeted communications.

The following activities are not within the scope of Contract Activities:

- Training of MDOC employees on the new COMS software system.

3. OCM Project Schedule

Deliverables	Apr-2019	May-2019	Jun-2019	Jul-2019	Aug-2019	Sep-2019	Oct-2019	Nov-2019	Dec-2019	Jan-2020	Feb-2020	Mar-2020	Apr-2020	May-2020	Jun-2020	Jul-2020
	All Milestones (All)			Food Service (FS)		Healthcare (HC)			Trust (TR)				Parole Board / Field Ops (FO/PB)	Meal Track (MT)		
Change Management Plan			All													
Knowledge Transfer Plan			All													
Change Network Document			All													
Communications Plan			All													
Readiness Survey Results (TGPS tool)			X	All		X	FS			X	HC			X, X	TR, FO/PB, MT	
Knowledge Transfer Scorecard					FS				HC					TR	FO/PB, MT	
Customized Stakeholder Action Plans				FS				HC				TR		FO/PB	MT	
Business Process Impact Tracker				FS				HC				TR		FO/PB	MT	
Facility Readiness Checklists & Dashboard					FS				HC					TR	FO/PB	
Communications Material Report						FS				HC					TR	

- Items placed on timeline above represent the month in which the Contractor will submit the applicable deliverable (+/- 4 weeks) to MDOC. The specific delivery dates will be included in Contractor Deliverable Tracker as described below.
- Fees associated with each deliverable will be assigned proportionally based on the overall fee structure outlined below in Section 9 and such fees will be detailed in the Contractor Deliverable Tracker.
- The use of “X” in the table above indicates when a TGPS Readiness Survey will begin. Each sequential survey will be cumulative, such that previously surveyed areas are re-surveyed to gauge ongoing success. Thus, after the Initial baseline survey and the initial Food Service survey, the subsequent initial Health Care survey will include a second Food Service survey. Likewise, the initial Trust, Field Operations/Parole Board, and Meal Tracking surveys will include a second Health Care survey and a third Food Service survey.
- Contractor will conduct knowledge transfer activities and provide TGPS survey results for Trust, FO/PB, and MT by June 12, 2020. However, the Contractor acknowledges that changes to the COMS project schedule (which occur from time to time) could result in some OCM activities falling out of the scope of this Statement of Work and therefore would be removed from Contract Activities by the Change Control Process.
- ★ represents an Invoice Date (Payment Milestone) and is further outlined below in section 4. Deliverables.

4. Deliverables

For each deliverable described below, Contractor will have the responsibility of completing the applicable task or deliverable and directing MDOC in a supporting role, such support being an essential element to Contractor’s ability to provide such deliverable.

Deliverables	Description	Deliverable Date
Empower Project to Lead		

Deliverables	Description	Deliverable Date
Change Management Plan	The Change Management Plan is a detailed plan provided in Word format that will: <ul style="list-style-type: none"> Outline the change management activities that will be completed for the COMS implementation. Confirm change management deliverables, timeline, methodology, and key resources. 	06/2019
Knowledge Transfer Plan	The Knowledge Transfer Plan, provided in Word format, lists the activities to effectively transfer knowledge from the Contractor to the MDOC team.	06/2019
Knowledge Transfer Scorecard	The Knowledge Transfer Scorecards, provided in Word format, lists the types of activities that could be performed by MDOC personnel.	08/2019; 12/2019; 05/2020; 06/2020
Engage Key Stakeholders		
Readiness Survey Results (Transformation GPS Tool)	The Readiness Survey Results are PDF documents of the results and Contractor's analysis of the on-line Transformation GPS survey that is submitted to MDOC employees five (5) times through the duration of the Project. (Contractor will also provide the State with all underlying data generated by State survey respondents in Excel format. This will include, but not be limited to, the results of each particularized question on each conducted survey.) <ul style="list-style-type: none"> Once at the onset of the OCM project to establish a baseline. 	07/2019
	<ul style="list-style-type: none"> Then at the following milestones: <ul style="list-style-type: none"> Food Service 	10/2019
	<ul style="list-style-type: none"> Health Care 	02/2020
	<ul style="list-style-type: none"> Trust 	06/2020
	<ul style="list-style-type: none"> Parole Board/FO and Meal Tracking 	06/2020
Customized Stakeholder Action Plans	Customized Stakeholder Action Plan is a Word document providing a high-level summary of impacts and engagement strategy for each group.	07/2019; 11/2019; 03/2020; 05/2020; 06/2020
Mobilize Change Network		
Change Network Document	The Change Network Document is a list of Change Champions provided in a Word format which details the roles and responsibilities, who in the organization will fill these roles, and what engagement will look like within the change network.	06/2019

Deliverables	Description	Deliverable Date
Facility Readiness Checklists & Dashboard	<p>The Facility Readiness Checklists & Dashboard are Excel documents for each facility that:</p> <ul style="list-style-type: none"> • Develop a list that outlines all readiness activities, tasks, etc., required of each facility to “be ready” for the COMS implementation. • Provides a dashboard with an overall view of the organization’s level of preparedness for the COMS implementation. 	08/2019; 12/2019; 05/2020; 06/2020
Understand Change Impacts		
Business Process Impact Tracker	<p>The Business Process Impact Tracker is an Excel document that:</p> <ul style="list-style-type: none"> • Documents where the biggest impacts will be on day-to-day work of the users, so that they can be emphasized in both communications and training. 	07/2019; 11/2019; 03/2020; 05/2020 06/2020
Communicate for Awareness and Understanding		
Communications Plan	<p>The Communications Plan is a detailed Word document that:</p> <ul style="list-style-type: none"> • Outlines the communications that will be completed, the communication events/ deliverables timeline, channels, and responsibilities. • Breaks down, in alignment to stakeholder readiness and change impact areas, the key messages, communication vehicle, intended audience, and timing for each type of communication. • Merges existing communication plans across the COMS project. • The communications materials are Word document(s) developed and delivered digitally approximately 2-3 per month that utilize existing MDOC communication channels (i.e. Corrections Connections newsletter, podcast, etc.) and are focused on the highest impacts to MDOC’s staff. Such materials also include the development of analog options such as posters, banners, pocket guides. 	06/2019
Communications Material Reports	<p>The Communication Materials Report is a Word Document that lists a summary of the Communication materials that were developed for a release.</p>	09/2019; 01/2020; 06/2020

5. Work Location

Contract Activities shall be performed within the greater Lansing area, at locations provided by MDOC. When appropriate, work will also be conducted onsite at specific facility locations, and offsite at Contractor locations.

6. Equipment Resources

For all Contract Activities performed on this Project, the tools required to access MDOC systems for this engagement, include work space for four Contractor personnel which shall be provided by MDOC to Contractor.

7. Project Team

Contract Activities will be led by Contractor Senior Manager, Gregg Bourdo, supported by the following Contractor resources:

Role	Name	Start Date	End Date
Engagement Lead	Gregg Bourdo	4/15/2019	6/12/2020
OCM Manager	Denise Eggleston	4/15/2019	6/12/2020
OCM Manager	Maurice Sessoms	4/15/2019	6/12/2020
OCM Analyst	Trajan Centers	4/15/2019	6/12/2020

The Project will be under the control of the MDOC Project Control Office. Minimally, the State agrees to provide the following support:

Role	Name	Start Date	End Date	Time Allocation
OCM Contractor Support	TBD	4/15/2019	6/12/2020	25 - 40% (duration of Project)

8. Assumptions and Obligations

In addition to any other responsibilities or assumptions described in this SOW or the Contract, the following is a list of the obligations for which MDOC will be responsible, conditions on Contractor's performance, and assumptions upon which Contractor relies in agreeing to perform the Contract Activities (collectively "MDOC's Obligations"). If any of MDOC's Obligations are not performed or prove to be incorrect, it may cause changes to Contractor's delivery schedule, fees and expenses, deliverables, level of effort required, or otherwise impact Contractor's performance of the Contract Activities and Contractor shall have no liability with respect to its inability to perform the Contract Activities, unless remedied pursuant to the Contract Change Notice process outlined in Section 54 of Contract's Standard Contract Terms.

- Decisions to be made by MDOC and Contractor will be made on a timely basis.
- MDOC will provide reasonable on-site work areas for Contractor personnel with access to the specific MDOC environments, information, and tools as may be reasonably required throughout the course of Contractor's performance under this SOW.
- MDOC will manage the performance of MDOC resources and other third-party contractors or vendors engaged by MDOC, even if Contractor has been involved in recommending or selecting such contractors or vendors, or in the monitoring of their work. MDOC will be responsible for the contractual relationship with such third parties and for their commercially reasonable cooperation with Contractor.
- MDOC will be responsible for determining if and how it will implement any recommendations made by Contractor. It is MDOC's sole responsibility to act or refrain from acting on the analysis, results and/or recommendations provided to it by Contractor.

- MDOC acknowledges that while Contractor’s personnel working hereunder may, through experience or specialized training or both, be familiar with the general regulatory environment in their capacity as information technology and management consulting professionals, that none of Contractor, its affiliates, personnel or subcontractors are licensed, certified and/or registered in any jurisdiction as accounting, auditing, bookkeeping, tax advisory professionals, and will not be required to provide any regulatory, legal or financial advice, including (but not limited to) performing any compliance activities or reporting directly to a state or any instrumentality thereof, including regulatory agencies on behalf of MDOC or the State of Michigan generally.
- MDOC shall be responsible for obtaining, at no cost to Contractor, consents for Contractor’s use of any third-party products, including, but not limited to software (including purchase of any licenses), necessary for Contractor to perform its obligations under this SOW.
- MDOC understands and agrees that MDOC will be responsible for determining whether the Contract Activities provided by Contractor hereunder, including any revised business processes implemented pursuant to this SOW: (i) meet MDOC’s business requirements; (ii) comply with all federal, state and local laws, ordinances, codes, regulations and policies; and, (iii) comply with MDOC’s applicable internal guidelines, long-term goals and any related agreements.
- MDOC will be responsible for all printing and related costs as such costs relate to Contract Activities.
- Contract Activities and Contractor obligations under this SOW are predicated on the following COMS project milestone schedule and material deviations from this schedule may prevent Contractor from fulfilling its obligations under this SOW.

Milestone	Production Begin*
Food Service	August 2019
Health Care	December 2019
Trust	May 2020
Field Operations/Parole Board	June 2020
Meal Tracking	July 2020

* MDOC’s COMS project schedule governs the production dates above. Any material changes to these dates will be assessed to determine impacts to OCM activities.

9. Personnel

Contractor must appoint one Project Manager/Contractor Representative, specifically assigned to this engagement, that will lead Contractor’s efforts and respond to State inquiries regarding the activities under the Contract and answering questions related to deliverables. This resource will report to the State Project Manager for purposes of this engagement.

The State of Michigan reserves the right to interview and approve any Project Manager/Contractor Representative or any other position that will involve direct contact with the State (“Key Personnel”). In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection. The State may require a 30-calendar day training period for replacement personnel.

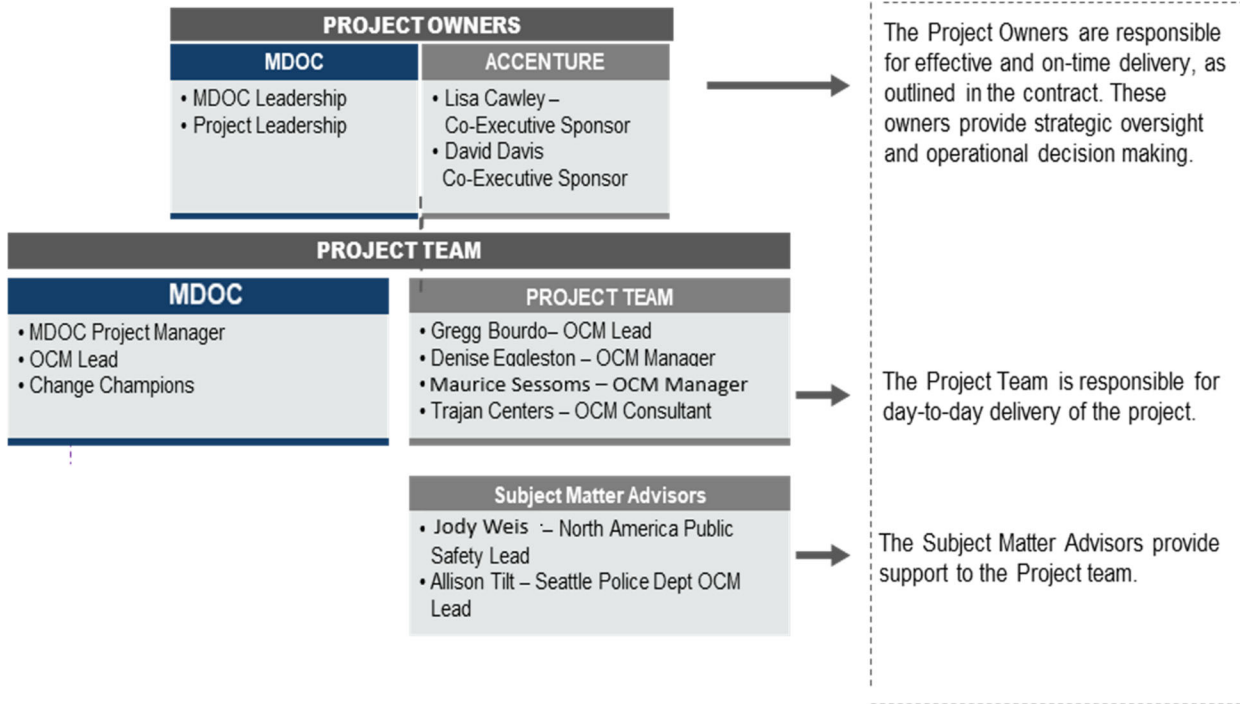
Contractor will not remove any Key Personnel from their assigned roles without the prior written consent of the State. Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("Unauthorized Removal"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of any resulting contract, in respect of which the State may elect to terminate the contract. It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of any resulting contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal.

Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under the Contract, Contractor will issue to the State the corresponding credits set forth below (each, an "Unauthorized Removal Credit"):

- (i) For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the credit amount will be \$25,000.00 per individual if Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30 calendar days before the Key Personnel's removal.
- (ii) If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 calendar days, in addition to the \$25,000.00 credit specified above, Contractor will credit the State \$833.33 per calendar day for each day of the 30 calendar-day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30 calendar days of shadowing will not exceed \$50,000.00 per individual.

Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any fees or other charges payable to Contractor under the Contract.

Contractor's staff will be assigned to this OCM project as outlined below in the organizational chart and are immediately available to fulfill their positions. Contractor's team includes both Michigan-based and out of state resources. Contractor will be onsite at MDOC either in Lansing or at specific facilities, as appropriate, for approximately 80% of the time.



10. Professional Fees

Contractor’s fees for this SOW shall be performed on a fixed fee basis as indicated in the table below. The total fees for Contract Activities shall not exceed Two Million and Two Hundred Thousand Dollars and forty-three cents (**\$2,200,000.43**):

Invoice Date	Amount
June 2019 (All Release Milestone)	\$550,000.00
August 2019 (Food Service Milestone)	\$333,012.75
December 2019 (Health Care Milestone)	\$222,366.00
May 2020 (Trust Milestone)	\$333,012.75
June 2020 (FO/Parole Board Milestone)	\$509,055.00
June 2020 (Meal Tracking Milestone)	\$252,553.93

11. Liquidated Damages

Late or improper completion of the Services or Deliverables will cause loss and damage to MDOC and it would be impracticable and extremely difficult to fix the actual damage sustained by MDOC. Therefore, if there is late or improper completion of the Services or Deliverables, MDOC is entitled to collect liquidated damages in the amount of \$5,000 and an additional \$100 per day for each day the Contractor fails to remedy the late or improper completion of the relevant Contract Activity.



STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management & Budget
 525 W. Allegan Street
 P.O. Box 30026
 Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **190000000477**

between

THE STATE OF MICHIGAN

and

CONTRACTOR	Accenture
	One Financial Plaza, 755 Main Street Suite 1600
	Hartford, CT 06103
	Lisa Cawley
	589-248-1187
	Kathleen.Cawley@Accenture.com
	CV0062320

STATE	Program Manager	Jeff Anderson	MDOC
		517-335-1251	
		AndersonJ30@michigan.gov	
STATE	Contract Administrator	Steve Rigg	DTMB
		517-249-0454	
		RiggS@Michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Organizational Change Management (OCM) for Offender Management System (COMS) - MDOC			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
April 5, 2019	December 31, 2020	1 – 1 year option	December 31, 2020
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
THIS IS NOT AN ORDER. This Contract Agreement is awarded on the basis of the State's inquiring RFP No. 190000000746. Orders for services will be issued directly by Departments through the issuance of a Delivery Order Form.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$2,200,000.43

STATE OF MICHIGAN

Contract No. 190000000746
MDOC Change Management for COMS Application

SCHEDULE A STATEMENT OF WORK

SCOPE

Under the direction of the State Project Manager, the Contractor must lead efforts to achieve, at a minimum, the following as it relates to each module implementation of the COMS application statewide:

1. The development of and maintenance of a Statement of Work/Change Management Plan.
2. The facilitation and attendance at meetings with State resources.
3. The development and dissemination of multiple communication options that will allow the State to actively engage MDOC staff regarding COMS project milestones and the statewide rollout of the COMS application.
4. The development, deployment, collection, analysis, and interpretation of measurable criteria by which to evaluate the effectiveness of communications, training, adoption of the COMS solution, and satisfaction with the COMS solution, including any identified need for remediation efforts.
5. Guidance on best practices for training MDOC resources.
6. The tailored communication of general information about the COMS project that considers the unique nature of the various employee groups and locations within MDOC.
7. The tailored communication of details related to business process changes throughout MDOC that consider the unique nature of the various employee groups and locations within MDOC.
8. The collection, analysis, and interpretation of stakeholder feedback and suggestions from MDOC resources.
9. The production of regular reports and results to the COMS project team and COMS project stakeholders.
10. The creation of OCM skills sets for certain MDOC resources such that MDOC may continue OCM efforts in the absence of the Contractor. This must include training materials.
11. The licensing of Contractor software following the engagement for use by MDOC, if applicable.

OPTIONAL SERVICES TO BE CONSIDERED UNDER THIS CONTRACT

12. Training logistics (planning, scheduling, tracking completion of training for 14,000 State employees)
13. Training delivery (develop computer-based or other training materials, deliver instructor-led training)

Requirements

1. Acceptance

- 1.1. Pursuant to the Request for Proposal, #190000000746, posting date of January 23, 2019, the Contractor and the State of Michigan (the State) will develop and maintain a Statement of Work/Change Management Plan which will initially encompass, at a minimum, the scope described above.

Such a mutually acceptable plan will be negotiated within ten (10) business days of the execution of this Contract and will be premised on the scope described above. All work performed under the second tier Statement of Work is subject to the agreed upon Standard Contract Terms.

It is expressly acknowledged by both parties that payments under this Contract will not be approved or paid by the State until a mutually acceptable amended second tier Statement of Work is agreed upon by both parties. Both the Contractor and the State acknowledge that the Statement of Work initially included within this Contract is to be used solely for the purpose of guiding the parties during the negotiation of an amended Statement of Work following the execution of this Contract and this initial Statement of Work is not to be

considered inclusive of all requirements or assumptions that must be included in an amended Statement of Work.

2. Staffing

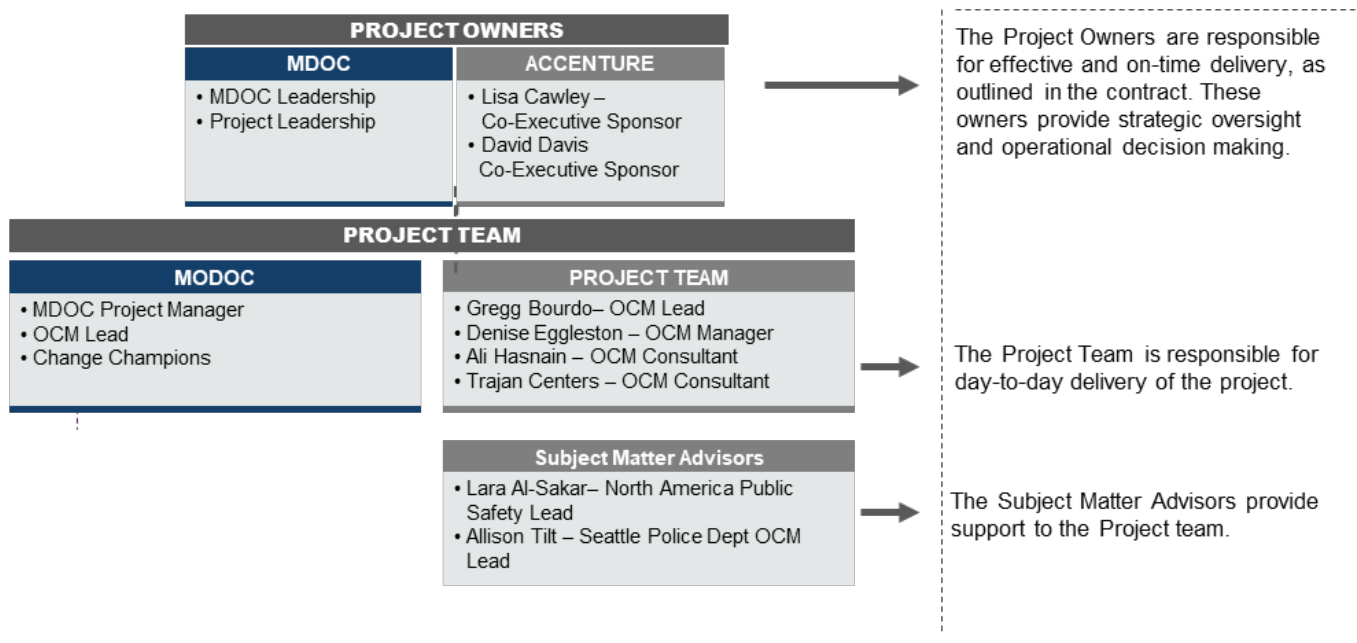
2.1. Contractor Representative

The Contractor appoints the following Contractor Representative, specifically assigned to State of Michigan accounts, that will respond to State inquiries regarding the Contract Activities, answering questions related to ordering and delivery, etc. (the “Contractor Representative”):

Lisa Cawley
 1001 Woodward Avenue, 4th Floor
 Detroit, MI 48226
 589-248-1187

Contractor’s staff will be assigned to this OCM project as outlined below in the organizational chart. **Contractor’s team includes both Michigan-based and out of state resources. Contractor will be onsite either in Lansing or at specific facilities, as appropriate, for ~ 80% of the time. Where appropriate, and in coordination with the MDOC project team, resources will either work offsite or at Contractor’s Detroit office.**

- **Kathleen (Lisa) Cawley** will be the Co-Executive Sponsor for this project and is based out of the Contractor’s Detroit office.
- **David Davis** will also be the Co-Executive Sponsor for this project and is located out of the Contractor’s Philadelphia office. The day-to-day operations of the project will be managed by the OCM Lead.
- **Gregg Bourdo** will be the OCM lead and is based out of Contractor’s Columbus office. Mr. Bourdo will be supported by three additional OCM resources
- **Denise Eggleston** will be an OCM resource supporting Gregg out of Contractor’s Raleigh office
- **Ali Hasnain** will be an OCM resource supporting Gregg based out of Contractor’s Detroit office.
- **Trajan Centers** will be an OCM resource supporting Gregg based out of Contractor’s Detroit office.
- **Lara Al-Sakar** will be the Contractor’s Public Safety Subject Matter advisor providing support to the team remotely.
- **Allison Tilt** will be the Contractor’s Public Safety Subject Matter advisor providing support to the team remotely.



STATE OF MICHIGAN
MDOC Change Management for COMS Application

SCHEDULE B
PRICING

1. Quick payment terms: 0 % discount off invoice if paid within N/A days after receipt of invoice.
2. The Contractor must provide pricing for each milestone completed. The cost calculation is all-inclusive for all costs associated with any resulting contract.
3. Price is firm-fixed for the term of the Contract. Actual dates will be finalized during the initial 10 days of this contract during development of second level Statement of Work.

Milestone	Estimate Number of End Users	Internal Consumers (Review Records and Complete Reporting)	External Consumers (Review Records and Complete Reporting)	Estimate Testing Begins	Estimated Production Rollout Begins	Estimated Production Rollout Ends	Not to Exceed Amount per Milestone not to exceed 14 Months
Food Service	300	Less than 50	N/A	5/14/19	8/2/19	9/10/19	\$ 444,017.03
Trust	400	1,000	N/A	5/17/19	8/6/19	9/17/19	\$ 444,017.03
Meal Tracking	6,500	500	N/A	TBD	TBD	TBD	\$ 336,738.37
Medical (Phase 1)	500	250	N/A	5/9/19	11/18/19	12/23/19	\$ 296,487.67
Parole Board/FO	1,700	250	2,000	12/18/19	4/17/20	5/20/20	\$ 678,740.34



STATE OF MICHIGAN

STANDARD CONTRACT TERMS

This STANDARD CONTRACT (“**Contract**”) is agreed to between the State of Michigan (the “**State**”) and Accenture LLP (“**Contractor**”), an Illinois limited liability partnership. This Contract is effective on April 5, 2019 (“**Effective Date**”), and unless terminated, expires on December 31, 2020.

This Contract may be renewed for up to one (1) additional one (1) year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via Contract Change Notice.

The parties agree as follows:

- 1. **Duties of Contractor.** Contractor must perform the services and provide the deliverables described in **Schedule A – Statement of Work** (the “**Contract Activities**”). An obligation to provide delivery of any commodity is considered a service and is a Contract Activity.

Contractor must furnish all labor, equipment, materials, and supplies necessary for the performance of the Contract Activities, and meet operational requirements, as specified in **Schedule A – Statement of Work**.

Contractor must: (a) perform the Contract Activities in a timely, professional, and workmanlike manner consistent with standards in Contractor’s trade, profession, or industry; (b) meet or exceed the performance and operational standards and specifications as provided in the Contract; (c) provide all Contract Activities in good quality, with no material defects; (d) not interfere with the State’s operations; (e) obtain and maintain all necessary licenses, permits or other authorizations necessary for Contractor’s performance of the Contract; (f) reasonably cooperate with the State, including the State’s quality assurance personnel, and any third party to achieve the specifications and objectives agreed in the Contract; (g) return to the State any State-furnished equipment or other resources in the same condition as when provided when no longer required for the Contract; (h) not make any media releases without prior written authorization from the State; (i) comply with all State physical and IT security policies and standards which will be made available upon request; and (j) provide the State priority in performance of the Contract except as mandated by federal disaster response requirements. Any breach under this paragraph is considered a material breach.

Contractor must also be clearly identifiable while on State property by wearing identification issued by the State, and clearly identify themselves whenever making contact with the State.

- 2. **Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

<p>If to State: Jeff Anderson 206 East Michigan Avenue Lansing MI 48933 AndersonJ30@Michigan.gov</p>	<p>If to Contractor: Kathleen Cawley 1001 Woodward Ave., 4th Floor Detroit, MI 48226 Kathleen.cawley@accenture.com (859) 248-1187</p>
--	---

3. **Contract Administrator.** The Contract Administrator for each party is the only person authorized to modify any terms of this Contract, and approve and execute any change under this Contract (each a “**Contract Administrator**”):

State:	Contractor:
Steve Rigg 525 W. Allegan St. Lansing, MI 48909 RiggS@Michigan.gov 517-249-0454	Kathleen Cawley 1001 Woodward Ave., 4th Floor Detroit, MI 48226 kathleen.cawley@accenture.com (859) 248-1187

4. **Program Manager.** The Program Manager for each party will monitor and coordinate the day-to-day activities of the Contract (each a “**Program Manager**”):

State:	Contractor:
Darren Elliott 206 East Michigan Avenue Lansing, MI 48933 ElliottD6@Michigan.gov	Gregg Bourdo 400 W. Nationwide Blvd Columbus, OH 43215 gregg.bourdo@accenture.com 330-608-3203

5. **Reserved.**

6. **Insurance Requirements.** Contractor must maintain the insurances identified below during the term of this Contract and is responsible for all deductibles. All required insurance must: (a) protect the State as additional insured and joint loss payee as required below from claims that may arise out of, are alleged to arise out of, or result from Contractor’s or a subcontractor’s performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
<u>Minimal Limits:</u> \$1,000,000 Each Occurrence Limit \$1,000,000 Personal & Advertising Injury Limit \$2,000,000 General Aggregate Limit \$2,000,000 Products/Completed Operations	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 0.
Umbrella or Excess Liability Insurance	
<u>Minimal Limits:</u> \$5,000,000 General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds.
Automobile Liability Insurance	
<u>Minimal Limits:</u> \$1,000,000 Per Occurrence	Contractor must have their policy: (1) endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds; and (2) include Hired and Non-Owned Automobile coverage.

Workers' Compensation Insurance	
<u>Minimal Limits:</u> Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
<u>Minimal Limits:</u> \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease.	
Crime (Fidelity) Insurance	
<u>Minimal Limits:</u> \$1,000,000 Employee Theft Per Loss	Contractor must have their policy: (1) cover forgery and alteration, theft of money and securities, robbery and safe burglary, computer fraud, funds transfer fraud, money order and counterfeit currency, and (2) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as Joint Loss Payees.
Professional Liability (Errors and Omissions) Insurance	
<u>Minimal Limits:</u> \$4,000,000 Each Occurrence \$4,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, including: (1) unauthorized access or use of a computer system or network, (2) denial of service attacks, (3) receipt or transmission of malicious code, (4) failure to protect confidential, personal or corporate information, (5) wrongful collections of confidential, personal, or corporate information, (6) violation of privacy laws, statutes, or regulations in connection with an event described in (4) or (5) above, and (7) media liability.

If any of the required policies provide **claims-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this **Section**; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by general liability, automobile liability, and workers compensation insurance. Failure to maintain the required insurance does not limit this waiver.

This **Section** is not intended to and is not be construed in any manner as waiving, expanding, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

- 7. Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made by check payable to the State of Michigan and mailed to:

Department of Technology, Management and Budget
Cashiering
P.O. Box 30681
Lansing, MI 48909

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

- 8. Extended Purchasing Program.** This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal. Upon written agreement between the State and Contractor, this contract may also be extended to: (a) State of Michigan employees and (b) other states (including governmental subdivisions and authorized entities).

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

- 9. Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations, and liabilities set forth in this Contract. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Contractor hereby acknowledges that the State is and will be the sole and exclusive owner of all right, title, and interest in the deliverables that Contractor creates for delivery to the State (the "**Deliverables**") and all associated intellectual property rights, if any, except for Contractor Technology. Except for Contractor Technology, such Deliverables and related intellectual property are works made for hire as defined in Section 101 of the Copyright Act of 1976. To the extent any Deliverables and related intellectual property do not qualify as works made for hire under the Copyright Act, Contractor will, and hereby does, immediately on their creation, assign, transfer and otherwise convey to the State, irrevocably and in perpetuity, throughout the universe, all right, title and interest in and to the Deliverables, including all intellectual property rights therein, and grants to the State a non-exclusive, paid-up, right and license to use, irrevocably and in perpetuity, for the State's purposes, any Contractor Technology included in the Deliverables. Except for the foregoing license grant, Contractor or its licensors retain all rights in and to all Contractor Technology. "**Contractor Technology**" means all works of authorship, materials, information and other intellectual property created prior to or independently of the performance of the Contract Activities, or created by Contractor or its subcontractors as a tool for their use in performing the Contract Activities plus any modifications or enhancements thereto and derivative works based thereon. Each party is otherwise free to use concepts, techniques, and know-how retained in the performance or receipt of the Services. Contractor is not precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the Deliverables provided and to the extent that they do not contain State Confidential Information.

- 10. Subcontracting.** Contractor may not delegate any of its obligations under the Contract without the prior written approval of the State. Contractor must notify the State at least 30 calendar days before the proposed delegation,

and provide the State any information it requests to determine whether the delegation is in its best interest. If approved, Contractor must: (a) be the sole point of contact regarding all contractual matters, including payment and charges for all Contract Activities; (b) make all payments to the subcontractor; and (c) incorporate the terms and conditions contained in this Contract in any subcontract with a subcontractor. Contractor remains responsible for the completion of the Contract Activities, compliance with the terms of this Contract, and the acts and omissions of the subcontractor. The State, in its reasonable discretion, may require the replacement of any subcontractor.

- 11. Staffing.** The State's Contract Administrator may require Contractor to remove or reassign personnel by providing a notice to Contractor. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot promptly replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.
- 12. Background Checks.** Contractor must perform background checks on all its employees and subcontractors and its employees prior to their assignment. Only Contractor or its vendor will: (i) conduct the background checks or (ii) have access to the results. Contractor will: (i) not assign anyone who does not pass the background check to any State project under this Contract and (ii) certify to the State the compliance with the process. The scope of a background check is at the discretion of the State. Contractor is responsible for all costs associated with the requested background checks.
- 13. Assignment.** Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.
- 14. Change of Control.** Contractor will notify, at least 90 calendar days before the effective date, the State of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following: (a) a sale of more than 50% of Contractor's stock; (b) a sale of substantially all of Contractor's assets; (c) a change in ownership through a transaction or series of transactions; (d) consummation of a merger or consolidation of Contractor with any other entity; (e) or the board (or the stockholders) approves a plan of complete liquidation. A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.
- 15. Ordering.** Contractor is not authorized to begin performance until receipt of authorization as identified in **Schedule A – Statement of Work**.
- 16. Acceptance.** Contract Activities are subject to review by the State as set forth in this Section ("**State Review Period**"). For written Deliverables of 100 pages or less, the State Review Period is 5 business days. For written Deliverables of more than 100 pages, the State Review Period is 10 business days. The State requires a review of all draft Deliverables. If the Contract Activities are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Contract Activities are accepted, but noted deficiencies must be corrected; or (b) the Contract Activities are rejected. If the State finds material deficiencies, it may: (i) reject the Contract Activities without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 23, Termination for Cause**. If the State fails to provide notice to Contractor of acceptance, acceptance with noted deficiencies, or rejection of the Contract Activities within the State Review Period, or fails to meet its obligations under this Section, and such delay or failure prevents Contractor from meeting deadlines that are dependent upon receipt of such notice, within 5 calendar days of the end of the State Review Period, the Contractor may request a reasonable extension of those deadlines. Upon such a request, the State must grant an extension of affected deadlines directly affected by the State's delay, which must match the number of days the State's notice was late, unless otherwise agreed to by the parties. All such extensions must be documented via Contract Change Notice to become effective.

Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Contract Activities, Contractor must cure, at no additional cost, the deficiency and deliver

unequivocally acceptable Contract Activities to the State. If acceptance with deficiencies or rejection of the Contract Activities impacts the content or delivery of other non-completed Contract Activities, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract. If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the Contract in whole or in part. The State, or a third party identified by the State, may perform the Contract Activities and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

17. Reserved.

18. Reserved.

19. Reserved.

20. Terms of Payment. Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in **Schedule A - Statement of Work**. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the State's exclusive use. Notwithstanding the foregoing, all prices are inclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Contract Activities. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

21. Liquidated Damages. Liquidated damages, if applicable, will be set forth in **Schedule A - Statement of Work**. The State may assess liquidated damages for late or improper completion of Contract Activities due to Contractor's acts or omissions (and not due to circumstances outside of Contractor's control). Liquidated damages are subject to the cap set forth in **Section 28, Limitation of Liability**.

22. Stop Work Order. The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the factual basis for such suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate the Contract or purchase order. The State will not pay for Contract Activities, Contractor's lost profits, or any additional compensation during a stop work period.

23. Termination for Cause.

- a. The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:
 - (a) endangers the value, integrity, or security of any location, data, or personnel;
 - (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor;
 - (c) engages in any misconduct during the course of the Contract Activities that may expose the State to liability;
 - (d) breaches any of its material duties or obligations; or
 - (e) fails to cure a material breach within five (5) business days or as specified in a notice of breach, whichever is longer. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

- b. If the State terminates this Contract under this **Section**, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately or (b) continue to perform for a specified period (either one being the "**Cause Termination Date**"). If it is later determined that Contractor was not in breach of the Contract, the termination will be deemed to have been a Termination for Convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 24, Termination for Convenience**.
- c. The State will only pay for amounts due to Contractor for Services rendered up to the Cause Termination Date and Deliverables accepted by the State on or before the Cause Termination Date, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Contract Activities from other sources.

24. Termination for Convenience. The State may terminate this Contract in whole or in part without penalty and for any reason, including but not limited to, appropriation or budget shortfalls, with five (5) business days' written notice to Contractor (the "**Convenience Notice Period**"), provided, however that in the event of a budget shortfall or legislative or executive action that fails to appropriate funds for this Contract (each a "**Non-Appropriation Event**"), the State may terminate this Contract by providing notice within a reasonable timeframe after such Non-Appropriation Event. The termination notice will specify whether Contractor must: (a) cease performance of the Contract Activities at the end of the Convenience Notice Period or (b) continue to perform the Contract Activities in accordance with **Section 25, Transition Responsibilities** (the "**Convenience Termination Date**"). If the State terminates this Contract for convenience, the State will pay for all (a) Services rendered, Deliverables accepted, and allowable costs/expenses as of the Convenience Termination Date and (b) all reasonable costs, as determined by the State, for State approved Transition Responsibilities. Notwithstanding the foregoing, if the State terminates this Contract for a Non-Appropriation Event, the State will pay the Contractor for the above costs only to the extent funds are available.

25. Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract Activities to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Contract Activities to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Contract Activities at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Contract Activities, reports and other documentation, to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and Confidential Information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed Deliverables prepared under this Contract as of the Contract termination date; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). If the State requests Contractor to provide transition assistance that exceeds the scope of subsections (a) through (e) above, the parties must mutually agree to such work. This Contract will automatically be extended through the end of the transition period.

26. General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all third party actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any intellectual property right or other right of any third party (an "**Infringement Claim**"); (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to tortious action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of

them may be liable). Contractor will have no liability, however, to the State under this **Section** to the extent that the Infringement Claim is based upon: (I) modifications to any item made by the State without the prior knowledge and approval of the Contractor in a manner that causes the infringement; (II) use of any item in combination with any hardware, software, or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item as reflected in this Contract; (III) the failure of the State to use corrections or enhancements to such item that are made available by Contractor, provided Contractor has given the State written notice of such correction or enhancement and such correction or enhancement will not negatively impact the item; (IV) Contractor's compliance with designs, specifications or direction provided by the State, but only if Contractor has provided notice to the State that the State's designs, specifications, or direction may give rise to an infringement claim; or (V) use of the item for other than its intended use as reflected under this Contract.

The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the reasonable satisfaction of the State, demonstrate its financial ability to carry out these obligations.

The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel at the State's sole expense; and to (iv) retain control of the defense if the State deems necessary. Contractor will not, without the State's written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this **Section**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27. Infringement Remedies. If, in either party's opinion, any Deliverables supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the equipment, software, commodity, or Deliverable, or if this option is not reasonably available to Contractor, (b) replace or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

28. Limitation of Liability and Disclaimer of Damages.

- (A) **DISCLAIMER OF DAMAGES.** Neither party will be liable for consequential, incidental, indirect, or special damages, including lost profits or lost business opportunities, regardless of the nature of the action.
- (B) **LIMITATION OF LIABILITY.** IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.
- (C) Exceptions. Subsections (A) and (B) above do not apply to:
 - a. Contractor's obligation to indemnify under **Section 26, General Indemnification**, except that claims made under **Section 26(d)** [Indemnity for acts and omissions] for direct or indirect damages, in the aggregate, shall be capped at the maximum amount of fees payable under this Contract;
 - b. Contractor's obligations under **Section 31, State Data**;
 - c. Damages arising from either party's recklessness, bad faith, or intentional misconduct.

29. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 28 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding that may negatively impact Contractor's performance or delivery of the Contract Activities (collectively, "Proceeding") involving Contractor, a subcontractor, or an officer or director of Contractor or subcontractor, that arises during the term of the Contract, which could include: (a) a criminal Proceeding; (b) a parole or probation Proceeding; (c) a Proceeding under the Sarbanes-Oxley Act; (d) a civil Proceeding involving: (1) a claim that might reasonably be expected to adversely

affect Contractor's viability or financial stability; or (2) a governmental or public entity's claim or written allegation of fraud; or (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract. Proceedings that are confidential under law are exempt from the foregoing disclosure requirement.

30. Reserved.

31. State Data.

- (A) Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes: (a) the State's data collected, used, processed, stored, or generated as the result of the Contract Activities; (b) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Contract Activities, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and, (c) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Contract Activities, which is defined under the Health Insurance Portability and Accountability Act (HIPAA) and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This **Section** survives the termination of this Contract.
- (B) Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Contract Activities, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Contract Activities. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Contract Activities, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This **Section** survives the termination of this Contract.
- (C) Extraction of State Data. Contractor must, within five (5) business days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of the State Data in the format specified by the State.
- (D) Backup and Recovery of State Data. Unless otherwise specified in **Schedule A - Statement of Work**, Contractor is responsible for maintaining a backup of State Data and for an orderly and timely recovery of such data. Unless otherwise described in **Schedule A - Statement of Work**, Contractor must maintain a contemporaneous backup of State Data that can be recovered within two (2) hours at any point in time.
- (E) Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than

twenty-four (24) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination. The parties agree that any damages relating to a breach of this **Section** are to be considered direct damages and not consequential damages. This **Section** survives termination or expiration of this Contract.

32. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. The provisions of this **Section** survive the termination of this Contract.

- a. Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.
- b. Obligation of Confidentiality. The parties agree to exercise reasonable care in keeping all Confidential Information confidential, to protect the Confidential Information of the disclosing party in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care, and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. Disclosure of Confidential Information to a subcontractor is also permissible if required by law, regulation, or court order, provided that the disclosing provides the other party with notice of the legal request within one (1) business day of receipt and the

parties assist each other in seeking legal relief as appropriate. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this **Section**.

- c. Cooperation to Prevent Disclosure of Confidential Information. Each party must use its commercially reasonable efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party promptly in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.
- d. Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek to obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Contract Activities corresponding to the breach or threatened breach.
- e. Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control; provided, however, that Contractor must return State Data to the State following the timeframe and procedure described further in this Contract. Should Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and must certify the same in writing within 5 calendar days from the date of termination or expiration to the other party. However, the State's legal ability to destroy Contractor data may be restricted by its retention and disposal schedule, in which case Contractor's Confidential Information will be destroyed after the retention period expires. Notwithstanding anything herein to the contrary, Contractor may retain copies of Non-State Data, and any summaries, analyses, notes, or extracts prepared by Contractor which are based on or contain portions of Confidential Information to the extent necessary to evidence performance of the Services, in no event to exceed the Audit Period set forth in **Section 36** below, provided that Contractor retains such copies in accordance with its confidentiality obligations hereunder.

33. Data Privacy and Information Security.

- a. Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality and security as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is reasonably designed to: (a) provide for the security and confidentiality of the State Data; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of State Data; (c) protect against unauthorized disclosure, access to, or use of State Data; (d) ensure the proper disposal of State Data; and (e) enable compliance by all employees, agents, and subcontractors of Contractor, if any, with all of the foregoing. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable State IT policies and standards, which are available to Contractor upon request.
- b. **Reserved.**
- c. Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Contract Activities and from time to time during the term of this Contract. During the providing of the Contract Activities, on an ongoing basis from time to time and with reasonable notice, the State, at its own expense, is entitled to perform, or to have performed by an agent that is not a competitor of Contractor, an on-site audit of Contractor's data privacy and information security program solely as it relates to the Contract Activities, so long as such audit

neither unreasonably disrupts Contractor's business, nor exposes any such auditors to confidential information of Contractor's other clients. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within 45 calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

d. **Reserved.**

e. **State's Right to Termination for Deficiencies.** The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section**.

34. Reserved.

35. Reserved.

36. Records Maintenance, Inspection, Examination, and Audit. The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State or its designee and the auditor general upon request, all financial and accounting records (other than Contractor's internal costs to provide services) related to the Contract through the term of the Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Audit Period, Contractor must retain the records until all issues are resolved.

Within 10 calendar days of providing notice, the State and its authorized representatives or designees (which are not competitors of Contractor) have the right to enter and inspect Contractor's premises or any other places where Contract Activities are being performed, and examine, copy, and audit all records (other than Contractor's internal costs to provide services or any confidential information of other clients of Contractor) related to the Contract Activities. Contractor must cooperate and provide reasonable assistance. If any financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of the Contract must be paid or refunded within 45 calendar days. This **Section** applies to Contractor and any entity that performs Contract Activities in connection with this Contract, including any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor of Contractor.

37. Warranties and Representations. Contractor represents and warrants: (a) Contractor is the owner or licensee of any Contract Activities that it licenses, sells, or develops and Contractor has the rights necessary to convey title, ownership rights, or licensed use; (b) all Contract Activities are delivered free from any security interest, lien, or encumbrance and will continue in that respect; (c) the Deliverables will not knowingly infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (d) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (e) the Contractor signatory has the authority to enter into this Contract; (f) all information furnished by Contractor in connection with the Contract fairly and accurately represents Contractor's business, properties, finances, and operations as of the dates covered by the information, and Contractor will inform the State of any material adverse changes; (g) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading; and that (h) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606. A breach of this **Section** is considered a material breach of this Contract, which entitles the State to terminate this Contract under **Section 23, Termination for Cause**. TO THE EXTENT PERMITTED BY LAW, THE CONTRACTOR EXPRESSLY DISCLAIMS ANY WARRANTIES NOT LISTED HEREIN.

38. Conflicts and Ethics. Contractor will uphold appropriate ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. To the best of Contractor's knowledge, there exists no undisclosed actual or potential conflict between Contractor and the State, and its Contract Activities under this Contract, and in the event of change in

either Contractor's private interests or Contract Activities under this Contract, Contractor will inform the State regarding possible conflict of interest which may arise as a result of the change. Contractor must immediately notify the State of any violation or potential violation of these standards. This **Section** applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

- 39. Compliance with Laws.** Each party must comply with all federal, state and local laws, rules and regulations in connection with this Contract applicable to their respective businesses and/or organization.
- 40. Reserved.**
- 41. State Printing.** All printing in Michigan must be performed by a business that meets *one* of the following: (a) have authorized use of the Allied Printing Trades Council union label in the locality in which the printing services will be performed; (b) have on file with the Michigan Secretary of State, a sworn statement indicating that employees producing the printing are receiving prevailing wages and are working under conditions prevalent in the locality in which the printing services will be performed; or (c) have a collective bargaining agreement in effect and the employees are represented by an operations that is not influenced or controlled by management.
- 42. Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and Executive Directive 2019-09, Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.
- 43. Unfair Labor Practice.** Under MCL 423.324, the State may void any Contract with a Contractor or subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.
- 44. Governing Law.** This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.
- 45. Non-Exclusivity.** Nothing contained in this Contract is intended nor will be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Contract Activities from other sources.
- 46. Force Majeure.** Neither party will be in breach of this Contract because of any failure to perform arising from any disaster or acts of god that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors that is not a force majeure event with respect to such subcontractor.
- 47. Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely, or fails to respond within 15 business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This **Section** does not limit the State's right to terminate the Contract.

- 48. Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.
- 49. Website Incorporation.** The State is not bound by any content on Contractor's website unless expressly incorporated directly into this Contract.
- 50. Entire Agreement and Order of Precedence.** This Contract, which includes **Schedule A – Statement of Work**, **Schedule B – Pricing**, and any other expressly incorporated schedules and exhibits, is the entire agreement of the parties related to the Contract Activities. This Contract supersedes and replaces all previous understandings and agreements between the parties for the Contract Activities. If there is a conflict between documents, the order of precedence is: (a) first, this Contract, excluding its schedules, exhibits, and **Schedule A – Statement of Work**; (b) second, **Schedule A – Statement of Work** as of the Effective Date; and (c) third, schedules expressly incorporated into this Contract as of the Effective Date. NO TERMS ON CONTRACTOR'S INVOICES, ORDERING DOCUMENTS, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE CONTRACT ACTIVITIES WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF THE CONTRACT ACTIVITIES REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.
- 51. Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.
- 52. Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.
- 53. Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.
- 54. Contract Modification.** This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.
- 55. Prison Rape Elimination Act of 2003 (PREA), 42 U.S.C. § 15601**
- a. The Contractor and the Contractor Personnel shall comply with the Final Rule implementing PREA, all applicable PREA standards (Schedule D – PREA Standards) and the agency's policies. The Contractor and Contractor Personnel shall make itself familiar with and at all times shall observe and comply with all PREA regulations that in any manner affect the performance under this Contract. Failure to comply with the PREA standards and related polices of the MDOC, if applicable to the Contract Activities, will be considered a breach of contract and may result in termination of the contract.
 - b. Contract Personnel who may have contact with prisoners must complete PREA training Program A - Correctional Facilities Administration (CFA) Security Regulations (Schedule C – Program A – CFA Security Regulations) prior to entrance in any MDOC Facility. Upon completion, Contractor Personnel shall submit a signed memorandum to the Contract Administrator documenting completion of the training and date of completion.
 - c. As is deemed necessary, the MDOC Contract Monitor or Program Manager will provide the Contractor with current copies of all PREA documents via email. Any revisions to the documents will be emailed to the Contractor throughout the Contract period, and the Contractor must comply with all documentation provided.

Schedule C – Program A – CFA Security Regulations



PROGRAM A

**CORRECTIONAL
FACILITIES
ADMINISTRATION (CFA)**

SECURITY REGULATIONS

August 2014

Table of Contents

Module Description.....	Page 3
Overview Of The Michigan Department Of Corrections	Page 4
Approval Prior To Entering A Correctional Facility	Page 8
Vehicles on CFA Facility Property	Page 15
Tools and Equipment	Page 18
Entrance Into And Exit Out Of The CFA Facility	Page 22
Personal Protection Devices (PPD)	Page 25
When Authorized Items Become Contraband	Page 28
Prisoner Contact- Sexual Abuse, Sexual Harassment, Overfamiliarity and Unauthorized Contact	Page 30
Emergencies	Page 39
Worksite Protocols	Page 41
Conclusion	Page 46

Module Description: This module provides standardized training and orientation training required for all contractors, vendors, skilled trades, construction workers, student interns and volunteers providing services at Correctional Facility Administration work sites. Topics included in this training program are searches, vehicles, tool control, contraband, prisoner contact, discriminatory harassment and emergencies.

Original Module Developers: *Contractual Workers Committee* Bonita Hoffner, Deputy Warden, LCF – Chairperson; Bryan Watson, Deputy Warden, ATF; Janette Price, Deputy Warden, MTU; Aaron Wemple, Assistant Deputy Warden, JCS; Steve Parks, Central Office Physical Plant; Joe Lemke, Central Office Training

Date Originally Developed - December 1998

Revisions Completed By: The Office of New Employee Training & Professional Development, Curriculum Unit with the assistance of Bonita Hoffner, Kevin Lindsey, Joe Lemke and Tom Mullaly.

Revised: August 2007; September 2010, April 2014

Target Audience: All contractors, vendors, skilled trades, construction workers, student interns and volunteers providing services at Correctional Facilities Administration work sites. Vendors who are under direct continuous supervision and/or escort are not required to attend this program.

Time Frame: Training time is 1 hour.

Materials Needed and Provided by The Facility: Computer with On-Line Training Access, Applicable Policies, Procedures and DOM's; Facility Operating Procedures.

Program Objective: At the completion of this training participants will have an understanding of security regulations necessary and that shall be followed when working in Michigan Department of Corrections work sites.

Overview of the Michigan Department of Corrections

THE MICHIGAN DEPARTMENT OF CORRECTIONS RESPONSIBILITY

The goal of the Michigan Department of Corrections is to provide the greatest amount of public protection while making the most efficient use of the State's resources. It meets its goal by ensuring that the state's judges and other criminal justice administrators have the broadest possible array of viable sentencing and sanctioning options, and by ensuring that appropriate supervision is maintained so that Michigan's neighborhoods, families and citizens can be protected.

Our vision is to protect the public and build trust within Michigan communities.

Our mission is to create a safer Michigan through effective offender management and supervision in our facilities and communities while holding offenders accountable and promoting their rehabilitation.

THE STRUCTURE

The Department gets its authority and the sources of influence on Department operations through the U.S. Constitution; Michigan Constitution and Michigan Compiled Law.

The Departments structure and direction for operations is provided through:

Administrative Rules, which interpret the laws for State Agencies.

Policy Directives (PD), which provide the Departments direction and focus.

Director's Office Memorandum (DOM), which are implemented as temporary policies when an immediate response is necessary in providing direction.

Operating Procedures (OP), which are written statements on how the policies are to be implemented.

The Director is the chief administrative officer of the Department and thus is responsible for the overall operation of the Department. The Director is appointed by the Governor.

The Department of Corrections is divided into Administrations. All correctional institutions operated by the Department are under the Correctional Facilities Administration (CFA), which is headed by a Deputy Director, who reports to the Chief Deputy Director and is responsible for the operation of all correctional institutions.

Each institution within the Correctional Facilities Administration (CFA) is administered by a Warden. The Warden is responsible for the overall operation of their institution.

In the absence of the Warden a designee will maintain responsibility over the operation of the institution.

For the purposes of this training we will refer to the Warden and their designee as the Facility Head.

Throughout this training we will frequently refer to the facility head, and policies. You know now that we are referring to the Warden or designee and the documents that give us our direction.

Approval Prior to Entering A Correctional Facility

APPROVAL PRIOR TO ENTERING A CORRECTIONAL FACILITY

Regardless of the purpose for entering a correctional facility, entry is only allowed when explicit approval has been given by the facility head. Paperwork should be filled out prior to coming on site.

Training must be completed in accordance with PD 02.05.100 New Employee Training Program and the current New Employee Training Plan.

The business that is being conducted, along with the type of contact that you will have with the offenders at a CFA facility will determine the necessary training that is required.

This program (Program A) is orientation training which is required for all contractors, vendors, skilled trades, construction workers, student interns and volunteers providing intermittent services.

Law Enforcement Information Network (LEIN) application and personal information is necessary in order to complete the approval process.

When applicable, an ID card is generated after being LEIN cleared by using the information from the form.

Regardless of the purpose for entering a correctional facility, only allowable items will be carried into and out of the facility. See OP

04.04.100 Gate Manifests and Attachment A, Allowable Items Without Gate Manifest.

According to PD 04.04.110, Contraband is property (items) which is not allowed on facility grounds by State law, Administrative Rule or Department policy or procedure.

Proper dress and equipment for duty while inside of a correctional facility is just as important as what is brought onto facility grounds and when left unattended can become contraband. Be sure not to leave items unattended and take everything out with you that you brought in.

Drugs and Alcohol are not to be brought onto state property, whether it is intended to be left in a vehicle or not.

Individuals who staff have a reasonable suspicion of their being under the influence of drugs and/or alcohol will not be allowed to enter into the facility.

Being “under the influence” is any behavior, actions, words, odor or other evidence which is indicative of an individual who is or has been using drugs and/or alcoholic beverages.

Reasonable suspicion is suspicion based on a specific fact or facts and rational inferences drawn from those facts, based upon the knowledge and experience of corrections staff.

Prescription and/or over the counter medications may be authorized to bring onto facility grounds as follows:

The allowable items list (Attachment A, OP 04.04.100) will describe what and how much over the counter medications are authorized.

Prescription medications may be allowable on facility grounds, but only with authorization as given by the facility head and an Administrative Manifest is required (See OP 04.04.100 – Gate Manifests).

Prescribed **medical marijuana is not** an allowable item even though it is prescribed.

All individuals entering onto correctional facility property are subject to search (See PD 04.04.110 Search and Arrests in Correctional Facilities). Anyone refusing to be searched will not be allowed entrance into the facility and will be asked to leave the property.

The Department's responsibility to manage and control the State's correctional facilities includes the duty to prevent contraband from entering those facilities.

Pursuant to MCL 800.281 et seq., it is a felony to bring any of the following items into a correctional facility or onto facility property where prisoners may have access to them without prior written permission of the Warden:

Any weapon, including a pocket knife, or other implement which may be used to injure another person or which may be used in aiding a prisoner to escape;

Any alcoholic beverage or poison, except that not more than two ounces of wine may be brought into a facility for use by a clergy member during religious ceremonies;

Any prescription drug or controlled substance without written certification of need from a licensed physician, except that prescription drugs and controlled substances may be brought into a correctional facility as medical supplies for that facility. The physician's written certification must include the name of the person prescribed the drug or controlled substance, the prescribed dosage and frequency, and the reason it was prescribed.

Controlled Substance is defined as a drug, substance, or immediate precursor as set forth in MCL 333.7201 to 333.7231, including heroin, cocaine, LSD, and marijuana.

In addition to those items prohibited by State law, Department policy prohibits other items from being brought into a correctional facility or on facility grounds.

Personal cellular telephones and pagers are prohibited.

Personal cellular telephones (PD 04.04.100 paragraph L.) are not permitted on facility grounds or regional offices except in a locked motor vehicle in designated parking areas and in secured areas designated by the Warden or the highest ranking supervisor of the regional office for this purpose (e.g., locked locker).

In the State of Michigan it is a felony to provide a cell phone to a prisoner under MCL 800.283a.

Audio or visual recording devices, including cameras, are prohibited unless approved by the Warden.

Tobacco products also are prohibited both inside a correctional facility and on facility grounds.

Visitors also are prohibited from bringing money into a correctional facility, except where allowed for use of vending machines.

Wardens may prohibit other items from being brought into their respective facilities; however, items may not be prohibited that are otherwise specifically allowed pursuant to Department policy.

Members of the public entering a correctional facility are subject to search in order to prevent the introduction of contraband. If a member of the public refuses to be searched, s/he will not be forced to submit unless a search warrant has been obtained, but entry into the secured area of the facility on that occasion shall be denied and s/he may be

required to leave the premises. A person subject to a clothed body search who is wearing clothing which prevents a thorough clothed body search also shall be denied entry and may be required to leave the premises.

Members of the Public are defined as visitors, volunteers, attorneys, contractors, elected state officials, and anyone else who is not an employee.

A pat-down search is defined as a brief manual and visual inspection of body surfaces, clothing, briefcases, and similar items. The only clothing items that may be required to be removed are outerwear (e.g., coats, jackets, hats) and shoes. All items shall be removed from pockets.

A clothed body search is defined as a thorough manual and visual inspection of all body surfaces, hair, clothing, wigs, briefcases, prostheses, and similar items and visual inspection of the mouth, ears, and nasal cavity. The only clothing items that may be required to be removed are outerwear (e.g., coats, jackets, hats), shoes, and socks; however, all items shall be removed from pockets.

All members of the public shall be required to walk through a screening device or submit to the use of a hand-held screening device prior to entering a CFA institution; however, this requirement may be waived by the Warden for anyone personally escorted by the Warden or his/her designee. Any personal property which is taken inside the security perimeter of a CFA institution shall be searched.

Vehicles on CFA Facility Property

VEHICLES ON CFA FACILITY PROPERTY

All vehicles that enter the property of a CFA facility must be properly licensed and registered.

All vehicles that enter the property and that are operated while at a CFA facility must be operated only by properly licensed and certified individuals.

All vehicles that are brought onto CFA facility grounds must be parked in authorized areas only.

If a vehicle is discovered in an area of the facility grounds which has been posted against trespassing, the vehicle and its occupants may be detained while the appropriate law enforcement agency is summoned.

All vehicles must be properly secured.

No keys left inside or outside of the vehicle.

Lockable doors and compartments.

Securable windows.

Vehicles entering in the security perimeter must have the steering wheel secured with a “Club” security device or similar device in accordance with the CFA facility operating procedure.

No unauthorized items are to be stored in the vehicle.

The appropriate law enforcement agency shall be called whenever a person is found to be in possession of a non-authorized alcoholic beverage, poisonous substance, controlled substance, prescription drug, or weapon(s).

Absolutely no weapons are to be carried onto facility grounds or left in a vehicle regardless of whether a valid CCW allows the weapon to be carried.

Vehicles are subject to search as follows:

If it is suspected that there is contraband in a vehicle on facility grounds that does not belong to an employee, the matter shall be referred to the appropriate law enforcement agency. Employees shall not search the vehicle.

Tools and Equipment

TOOLS AND EQUIPMENT

Each Correctional Facilities Administration (CFA) institution is required to control items transported through all pedestrian and vehicle entrances in order to reduce the risk of contraband being brought into the institution, to prevent theft of state property, and to provide a record system for all packages, supplies, and materials brought into or out of the institution.

Employees, vendors, contractors, and individuals engaged in official business carrying items not listed on the list of allowable items must obtain a Gate Manifest (CSJ-404) in order to bring those items through the gates of an institution. This gate manifest is intended for a one time through use.

In the event an item is authorized to be brought through the gates on a daily basis, an Administrative Manifest (CSJ-127) shall be used for this purpose.

A Warden/Deputy Warden may issue an Administrative Manifest to employees carrying authorized items through the gates of his/her facility.

No manifest will be issued for an item specifically prohibited by Department policy or procedure (e.g. cellular telephones, personal pagers, pocket knives).

All items being brought through the gates into the facility will be searched. This includes items carried in, and those being removed, from the secure perimeter.

The person to whom the manifest is issued must present it along with the transported items when entering or departing the secure perimeter.

The Department has a specific policy for tool control which categorizes tools into two categories, critical and dangerous tools. Tools must be used, accounted for, secured, and stored in accordance with PD 4.4.120 Tool Control.

Tools, tool boxes, and equipment of contract workers performing services inside an institution shall be inventoried and inspected prior to entry into and exit from the institution. Staff designated to escort workers within the facility shall ensure tools are controlled with proper security and safety procedures and work activities are confined to authorized areas.

Critical tools are as follows: Metal cutting tools, including hacksaws, metal cutting blades, chisels, files, bolt cutters, and pipe cutters. Powered hand tools, drills and drill bits. Portable jacks and hoists. Wrenches 14" in length or longer. Acetylene torches, cutting tips, gauges, torch parts, arc welders, plasma cutting equipment. Grinders, emery wheels and abrasive discs. Tubing, pipe and conduit benders. Utility and carpet knives. Explosively driven tools (e.g., ramset guns) and

ammunition. Ladders nine feet in height or higher. Wire cutters and other hand tools primarily designed to cut wire.

Dangerous tools are as follows: Hand tools readily usable or adaptable as weapons, escape equipment or to defeat locking or security systems. Examples include screwdrivers and pliers. Wrenches less than 14" in length. Ladders less than 9' in length. Emery cloth and sandpaper.

Electric grinders not in use shall be locked in place with power positively locked out.

Safe handling of tools and equipment by authorized, licensed and certified users is necessary to ensure everyone's safety.

OSHA/MIOSHA standards must be maintained.

Tools must be properly removed from a CFA facilities secured perimeter if storage is not available inside of the facility.

It is the responsibility of a company contracted to perform work at CFA facilities to provide MSDS for all chemicals that will be utilized while working at a facility.

Entrance Into and Exit Out of the CFA Facility

ENTRANCE INTO AND EXIT OUT OF THE CFA FACILITY

The facility head will ensure all individuals who are authorized entry into a correctional facility are advised of rules that they must follow while in the facility. The facility head may order any individual who disregards facility rules or the conditions under which entry was approved to immediately leave the facility.

Access is allowable only during approved days and hours of operation for contractors and their employees.

Access that is necessary outside of the approved days and times established for conducting business or completing the work requires special authorization from the facility head.

Use only authorized entrance and exit points into and out of the facility. Individuals who enter into and out of a CFA facility should use the main gate entrance.

Vehicle traffic that enters into and out of a CFA facility will use a sally port entrance. It is at these entrances that you will be registered and/or identified for entry. You and the items you take in or are bringing out will be searched at these points as well.

Staff escorts will be assigned, when necessary, at the point of entrance. You are to remain with the escort until you exit the facilities secured perimeter.

All areas of a CFA facility are restricted access areas except those which are specifically designated and authorized to complete the work you are there to do.

Utilizing authorized entrances/exits when entering or leaving buildings and work locations will aid in keeping workers out of restricted areas.

Consequences for non-compliance include being escorted off of the facility property and possibly having authorization for future access revoked by the facility head.

Persons found in restricted areas, on CFA facility property, without authorization may be arrested for trespassing under the trespassing laws relevant to corrections.

All workers who are expected on site should be present when they are expected. In the case of a no call/no show of expected workers, access may be denied.

Contact information will be provided when it is necessary for announcing delay's or absence of workers or work crews.

Overtime that is accrued by the facility to provide escorts for expected work within the facility may be charged to the contracted company when the schedule is not adhered to.

Personal Protection Devices (PPD)

PERSONAL PROTECTION DEVICES (PPD)

The purpose of a PPD is to offer access to an alarm system that alerts staff in the Control Center of the CFA facility that there is a problem and also provides a general location of where the PPD has been activated.

There are some facilities within CFA that do not require a PPD.

When a CFA facility provides a PPD, you will receive information on how to properly operate the PPD.

Generally a PPD has push button alert activation, a pull-pin alert activation or both.

Depending on the facilities operating procedure a PPD may or may not be issued.

CFA facilities require that the PPD be properly worn so that it does not become lost and so that it is accessible by the user.

A PPD is not to be left lying around any where inside or outside of the facility.

The PPD is issued at a designated point within a facility and is returned usually at the same point where it was issued.

PPD's are considered sensitive items and are accounted for on each shift; therefore, a PPD should not be removed from facility grounds for any reason.

Proper use of a PPD requires that it is only activated when staff assistance is necessary.

An emergency type situation can occur at any time while inside of a CFA facility. The following is a list of examples which constitutes an emergency:

Injury or illness,

Assault by a prisoner,

Becoming disoriented inside of the facility.

Areas covered with the PPD's ability to activate an alarm are determined by each facilities physical plant. Not all areas may be covered by PPD access. Information of this nature will be shared with each person that is required to wear a PPD.

When Authorized Items Become Contraband

WHEN AUTHORIZED ITEMS BECOME CONTRABAND

Any item that you bring into a CFA facility, which is either on the allowable items list or has been properly authorized using a Gate Manifest/Administrative Manifest, is considered contraband when accessed by an offender.

There are specific items which are brought into the facility for offenders only by using proper channels. Consequences of improper security and control of tools and equipment can include serious physical injury and in the most extreme case even death.

Tools and equipment can be utilized by offenders to commit assaults, attempt escapes or for use in conducting unauthorized activities.

Careful cleanup and accountability of ALL items, including residual parts and pieces that occur as a result of performing proper work procedures, is essential for everyone's safety.

Pick up all nails, screws, wires.

Clean up any broken glass.

Remove and discard binding straps.

Remove every item or properly discard all items in approved disposal containers that are brought inside of a secured perimeter.

**Prisoner Contact –
Sexual Abuse,
Sexual Harassment,
Overfamiliarity and
Unauthorized Contact**

Prison Contact - Sexual Abuse, Sexual Harassment, Overfamiliarity and Unauthorized Contact

The Michigan Department of Corrections is committed to ensuring the safe and humane treatment of prisoners and a safe environment for all prisoners. An important part of a safe and humane environment includes being free from sexual abuse and sexual harassment.

The Department enforces a zero tolerance standard for staff, contractual employees, and volunteers to engage in sexual abuse, sexual harassment and overfamiliarity with prisoners.

Sexual abuse is a term used to describe certain kinds of prohibited behavior. Sexual abuse includes non-consensual sexual acts and sexual harassment. Based upon an imbalance of power, sexual relationships between staff, contractual employees, and volunteers with a prisoner are NEVER consensual.

Sexual abuse of a prisoner by a staff member, contractor, or volunteer includes any of the following acts, with or without consent of the prisoner:

Sexual Conduct with Offender or Overly-Familiar or Unauthorized Conduct/Sexual Relationship

- (1) Contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) Contact between the mouth and the penis, vulva, or anus;

(3) Contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;

(4) Penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;

(5) Any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;

(6) Any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1) through (5) of this section;

(7) Any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of a prisoner, detainee, or resident, and (8) Voyeurism by a staff member, contractor, or volunteer which means an invasion of privacy of a prisoner for reasons unrelated to official duties, such as peering at a prisoner who is using a toilet in his or her cell to perform bodily functions; requiring a prisoner to expose his or her buttocks, genitals, or breasts; or taking images of all or part of a prisoner=s naked body or of a prisoner performing bodily functions.

Sexual Harassment

Verbal comments or gestures of a sexual nature to a prisoner by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

Reporting Requirements

Anyone who observes sexual abuse/sexual harassment or receives an allegation of sexual abuse/sexual harassment, must report it to the appropriate supervisor immediately.

In addition to the Department's policy requirement that all allegations of sexual abuse, including sexual harassment, must be reported the Department is also required by federal and state law to report sexual abuse to outside authorities.

Sexual activity against a prisoner which may constitute a felony shall be reported to appropriate law enforcement authorities. For example, Michigan law MCL 750.520c provides that employees, contractual employees, or volunteers who engage in sexual contact with prisoners can be charged with a felony, Criminal Sexual Conduct in the second degree.

All reported allegations of sexual abuse/sexual harassment, shall be referred to the Internal Affairs section for investigation. All allegations shall also be referred to the Michigan State Police or other appropriate

law enforcement agency for investigation in accordance with policy and law.

In addition to reporting incidents of sexual abuse to the Michigan State Police, the Department must report all allegations of sexual abuse to the county department of social services of the county in which the abuse is suspected of having or believed to have occurred.

A contractual employee or volunteer who engages in sexual abuse/sexual harassment will be prohibited from providing services within any Department correctional facility.

Remember:

Treat any suggestion or allegation of sexual assault, abuse, or contact as serious.

A report of sexual abuse by a prisoner is to be kept confidential and shared only according to policy and law.

Overfamiliarity or Unauthorized Contact

The Department also enforces a zero tolerance standard for staff, contractual employees, and volunteers to engage in overfamiliarity with prisoners.

Overfamiliarity involves staff, contractual employees, and volunteers engaging in, or attempting to engage in conduct likely to result in intimacy or a close personal relationship with a prisoner. The following

behavior between staff, contractual employees, and volunteers and prisoners is prohibited:

- a. Exchanging personal letters or gifts.
- b. Requesting or granting special favors.
- c. Discussing personal matters, unless specifically related to a prisoners case.
- d. Engaging in horseplay.
- e. Flirting.
- f. Addressing each other by first name or a nickname.

Overfamiliarity or Unauthorized Contact with an offender includes the following types of relationships and behaviors:

Engaging in overfamiliarity with an offender, or a family member or listed visitor of an offender.

Having a personal relationship with an offender, the offender's family, or visitors at the facility you are working. Where such cases arise that there is already a personal relationship established prior to working at the facility, this information must be disclosed to include the name, number and location of the offender.

Making contact with any offender, family member of an offender or a listed visitor of an offender outside the regular performance of the job.

Giving or receiving letters, money, personal mementos, telephone numbers, legal or other services to or from an offender or a family member or a listed visitor of an offender.

Conversation of a sexual or romantic nature. Sexual abuse or sexual harassment of an offender's family members or listed visitors.

Financial involvement with offenders, family members of offenders, or listed visitors.

Giving or receiving messages, pictures or goods.

If unavoidable contact is made with an offender, a family member of an offender or a listed visitor of an offender, such contact must be reported in writing to the facility head through proper channels.

Allowable contact is defined based on the type of work you are conducting at the CFA facility. Any contact outside of the work you are doing could be inappropriate contact.

Offenders may try to have a conversation with you through a fence or by yelling across the yard. DON'T DO IT.

Generally an offender will not attempt to have an inappropriate conversation when staff are around.

Reporting contact or attempts to contact is required at any time an offender attempts to have a conversation, asks you to do something for them, asks you to bring something to them or asks you to contact someone for them.

Consequences of unauthorized contact or overfamiliarity will lead to being escorted out of the facility and possibly not being able to work at any other Department facility.

If the overfamiliarity is deemed a felony, the case will be turned over to the Michigan State Police or other appropriate Law Enforcement Agency and could lead to prosecution and incarceration for up to 15 years in prison.

Do's and Don'ts of working in a CFA facility are as follows:

DO stay with your escorting staff member.

DO dress appropriately for your job:

- Clean shirt and pants
- Under garments worn
- Clothing which is loose fitting
- Clothing which does not expose

DO consider where you are working.

DO ask questions about everything.

DO report everything unusual or questionable.

DO refer visitors to staff if they ask questions.

Don't leave tools & equipment unsecured. Make sure tools are inventoried.

Don't talk or visit with prisoners.

Don't do anything if the emergency siren sounds. You will receive direction from staff on what action to take.

Don't come to the facility without proper identification.

Don't bring any controlled items such as, butane lighters, knives, liquor, weapons, ammunition, dice, cameras or anything else into the prison.

Don't give money, cigarettes or any other items to prisoners.

Don't accept gifts or take anything from prisoners.

Don't carry any items of mail into or out of the prison for any prisoners.

Don't enter any area of the prison without staff permission or escort.

Don't forget you may be searched at any time entering, exiting or while you are inside the prison.

Don't bring any of the following items to the prison in your vehicle: firearms, weapons, ammunition, liquor or cameras.

Don't leave your keys in your vehicle.

Don't leave your vehicle unsecured (unlocked) on prison property.

Don't attempt to enter or exit the prison at any place other than where you are instructed to do so by staff.

Don't smoke or (chew tobacco) on prison property.

Don't forget to ask for staff assistance if you don't understand any of these rules.

Emergencies

EMERGENCIES

Sirens sounding inside of a CFA facility indicate a number of situations depending on what the siren sounds like.

The procedures to follow when a siren is sounded will be issued to you from the facility you are working.

Staff will direct you on what to do and where to go.

Each CFA facility is required to conduct a siren test monthly which may require non-employee's of the facility to exit the secured perimeter. This will cause a "work stop" for a couple of hours when this occurs.

When medical emergencies occur you should report it verbally to the nearest staff member, activate your PPD or use a nearby telephone. Do not attempt to leave the area unless none of the options mentioned are available.

Work Site Protocols

WORKSITE PROTOCOLS

Harassment of any kind is not tolerated at any Department facility.

The definition that the Department recognizes as being discriminatory harassment is: Unwelcome advances, requests for favors, and other verbal or non-verbal communication or conduct (e.g., comments, innuendo, threats, jokes, pictures, and gestures) based on race, color, national origin, disability, sex, sexual orientation, age, height, weight, marital status, religion, genetic information or partisan considerations.

Forms of harassment include but are not limited to: discriminatory harassment and sexual harassment.

Consequences of harassment are both personal and professional. Such actions can lead to civil suits as well as felony convictions.

Reporting harassment (i.e. victim of or witness to) should be done through proper channels. Any supervisor at a CFA facility is trained in proper reporting of complaints.

Authorized break areas/restrooms are to be the only areas utilized by non-employees of CFA facilities. This will help to ensure that restricted areas are not visited by unauthorized personnel.

Telephones for personal and business use will be as directed by the facility head.

Health care staff is not available for the purpose of providing care to anyone at CFA facilities except offenders.

Onsite care is not authorized for use unless it is a life or death emergency.

Locations that are available within the community can be utilized in accordance with their policies and ambulance services, if necessary, will be utilized in accordance with their policies as well.

CFA facilities have a Warden and Administrators assigned to act as facility heads. The Warden is the facility head and when absent assigns their designee.

The facility head has full rights to the facility. Some of those rights include and are not limited to:

Revoking permissions.

Adjusting authorities.

Alter working hours and days.

All items and personnel that are allowed inside.

Tours are not allowed without explicit authorization.

Proper authority is necessary for all activities and items as well as personnel for entrance into, exit out of and while on the grounds of any facility.

The facility Inspector is the person of contact for all questions, concerns and approvals.

Contact information for key personnel of the facility should be made available while you are working at the CFA facility.

Work place safety is covered by Civil Service Commission Rule 2-20.

Rule 2-20 prohibits employees from (1) engaging in acts of violence and threats of violence and (2) possessing or carrying firearms or explosives unless expressly authorized by the appointing authority.

Rule 2-20 requires employees to report violations involving acts or threats of violence or possessing or carrying firearms or explosives. If an employee becomes aware of an act of violence or a threat of violence, the employee shall immediately report the act or threat to the appointing authority or the appointing authority's designee.

Consequences of violating Rule 2-20 will include being escorted from facility grounds, possibly not being approved for work at any Department facility and may be referred to the Michigan State Police or other appropriate Law Enforcement Agency which could lead to a felony conviction.

Health and Safety requirements.

The Department is required by OSHA/MIOSHA standards to ensure the safety of its employees be maintained in accordance with applicable standards.

Reporting violations, hazards, emergencies and concerns should be done through proper channels which begins with the CFA facility head.

Consequences of non-compliance to MIOSHA standards, Department rules and any other applicable entity will be determined based on the circumstances and the issue at hand as well as in accordance with the stated standards.

Conclusion

CONCLUSION

After completing this training it may seem as if there are so many rules to working inside a CFA facility that it may be intimidating. To simplify things remember these keys:

You are working inside of a correctional facility (a prison) where everything you say and do will be observed.

If you have contact with offenders, offender's families etc. outside of your regular job duties report it to your supervisor.

If you are unsure about anything ask a staff member for assistance.

Don't give or leave anything for an offender and don't take anything from an offender.

The remainder of the orientation program should be used to answer and/or clarify any questions and to address other issues which may be specific to a particular work site.

ACKNOWLEDGMENT

I acknowledge that I have received a copy of, have read, understand and agree to abide by the CFA Security Regulations and PREA Federal Register. If I have any questions, I will ask my supervisor/manager.

Print Employee Name

Employee Signature

Date

**PREA STANDARDS – FINAL
Adult Prisons and Jails**

TABLE OF CONTENTS

General Definitions

§ 115.5 – General Definitions..... 3

Definitions Related to Sexual Abuse

§ 115.6 –Definitions Related to Sexual Abuse 5

Prevention Planning

§ 115.11 – Zero tolerance of sexual abuse and sexual harassment; PREA coordinator. 7
§ 115.12 – Contracting with other entities for the confinement of inmates..... 7
§ 115.13 – Supervision and monitoring. 7
§ 115.14 – Youthful inmates..... 8
§ 115.15 – Limits to cross-gender viewing and searches. 8
§ 115.16 – Inmates with disabilities and inmates who are limited English proficient..... 8
§ 115.17 – Hiring and promotion decisions..... 9
§ 115.18 – Upgrades to facilities and technologies. 9

Responsive Planning

§ 115.21 – Evidence protocol and forensic medical examinations..... 9
§ 115.22 – Policies to ensure referrals of allegations for investigations..... 10

Training and Education

§ 115.31 – Employee training..... 10
§ 115.32 – Volunteer and contractor training. 11
§ 115.33 – Inmate education..... 11
§ 115.34 – Specialized training: Investigations. 12
§ 115.35 – Specialized training: Medical and mental health care. 12

Screening for Risk of Sexual Victimization and Abusiveness

§ 115.41 – Screening for risk of victimization and abusiveness..... 12
§ 115.42 – Use of screening information..... 13
§ 115.43 – Protective custody..... 13

Reporting

§ 115.51 – Inmate reporting..... 14
§ 115.52 – Exhaustion of administrative remedies..... 14
§ 115.53 – Inmate access to outside confidential support services..... 15
§ 115.54 – Third-party reporting. 15

Official Response Following an Inmate Report

§ 115.61 – Staff and agency reporting duties. 15

**PREA STANDARDS – FINAL
Adult Prisons and Jails**

§ 115.62 – Agency protection duties. 15
§ 115.63 – Reporting to other confinement facilities. 15
§ 115.64 – Staff first responder duties. 16
§ 115.65 – Coordinated response..... 16
§ 115.66 – Preservation of ability to protect inmates from contact with abusers. 16
§ 115.67 – Agency protection against retaliation. 16
§ 115.68 – Post-allegation protective custody. 17

Investigations

§ 115.71 – Criminal and administrative agency investigations. 17
§ 115.72 – Evidentiary standard for administrative investigations..... 17
§ 115.73 – Reporting to inmates. 17

Discipline

§ 115.76 – Disciplinary sanctions for staff. 18
§ 115.77 – Corrective action for contractors and volunteers. 18
§ 115.78 – Disciplinary sanctions for inmates. 18

Medical and Mental Care

§ 115.81 – Medical and mental health screenings; history of sexual abuse. 19
§ 115.82 – Access to emergency medical and mental health services..... 19
§ 115.83 – Ongoing medical and mental health care for sexual abuse victims and abusers..... 19

Data Collection and Review

§ 115.86 – Sexual abuse incident reviews. 20
§ 115.87 – Data collection. 20
§ 115.88 – Data review for corrective action..... 20
§ 115.89 – Data storage, publication, and destruction. 21

Audits

§ 115.93 – Audits of standards. 21

Auditing and Corrective Action

§ 115.401 – Frequency and scope of audits. 21
§ 115.402 – Auditor qualifications. 22
§ 115.403 – Audit contents and findings. 22
§ 115.404 – Audit corrective action plan..... 22
§ 115.405 – Audit appeals. 22

State Compliance

§ 115.501 – State determination and certification of full compliance. 23

PREA STANDARDS – FINAL
Adult Prisons and Jails

§ 115.5 General definitions.

For purposes of this part, the term—

Agency means the unit of a State, local, corporate, or nonprofit authority, or of the Department of Justice, with direct responsibility for the operation of any facility that confines inmates, detainees, or residents, including the implementation of policy as set by the governing, corporate, or nonprofit authority.

Agency head means the principal official of an agency.

Community confinement facility means a community treatment center, halfway house, restitution center, mental health facility, alcohol or drug rehabilitation center, or other community correctional facility (including residential re-entry centers), other than a juvenile facility, in which individuals reside as part of a term of imprisonment or as a condition of pre-trial release or post-release supervision, while participating in gainful employment, employment search efforts, community service, vocational training, treatment, educational programs, or similar facility-approved programs during nonresidential hours.

Contractor means a person who provides services on a recurring basis pursuant to a contractual agreement with the agency.

Detainee means any person detained in a lockup, regardless of adjudication status.

Direct staff supervision means that security staff are in the same room with, and within reasonable hearing distance of, the resident or inmate.

Employee means a person who works directly for the agency or facility.

Exigent circumstances means any set of temporary and unforeseen circumstances that require immediate action in order to combat a threat to the security or institutional order of a facility.

Facility means a place, institution, building (or part thereof), set of buildings, structure, or area (whether or not enclosing a building or set of buildings) that is used by an agency for the confinement of individuals.

Facility head means the principal official of a facility.

Full compliance means compliance with all material requirements of each standard except for *de minimis* violations, or discrete and temporary violations during otherwise sustained periods of compliance.

Gender nonconforming means a person whose appearance or manner does not conform to traditional societal gender expectations.

Inmate means any person incarcerated or detained in a prison or jail.

Intersex means a person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female. Intersex medical conditions are sometimes referred to as disorders of sex development.

Jail means a confinement facility of a Federal, State, or local law enforcement agency whose primary use is to hold persons pending adjudication of criminal charges, persons committed to confinement after adjudication of criminal charges for sentences of one year or less, or persons adjudicated guilty who are awaiting transfer to a correctional facility.

PREA STANDARDS – FINAL
Adult Prisons and Jails

Juvenile means any person under the age of 18, unless under adult court supervision and confined or detained in a prison or jail.

Juvenile facility means a facility primarily used for the confinement of juveniles pursuant to the juvenile justice system or criminal justice system.

Law enforcement staff means employees responsible for the supervision and control of detainees in lockups.

Lockup means a facility that contains holding cells, cell blocks, or other secure enclosures that are:

- (1) Under the control of a law enforcement, court, or custodial officer; and
- (2) Primarily used for the temporary confinement of individuals who have recently been arrested, detained, or are being transferred to or from a court, jail, prison, or other agency.

Medical practitioner means a health professional who, by virtue of education, credentials, and experience, is permitted by law to evaluate and care for patients within the scope of his or her professional practice. A “qualified medical practitioner” refers to such a professional who has also successfully completed specialized training for treating sexual abuse victims.

Mental health practitioner means a mental health professional who, by virtue of education, credentials, and experience, is permitted by law to evaluate and care for patients within the scope of his or her professional practice. A “qualified mental health practitioner” refers to such a professional who has also successfully completed specialized training for treating sexual abuse victims.

Pat-down search means a running of the hands over the clothed body of an inmate, detainee, or resident by an employee to determine whether the individual possesses contraband.

Prison means an institution under Federal or State jurisdiction whose primary use is for the confinement of individuals convicted of a serious crime, usually in excess of one year in length, or a felony.

Resident means any person confined or detained in a juvenile facility or in a community confinement facility.

Secure juvenile facility means a juvenile facility in which the movements and activities of individual residents may be restricted or subject to control through the use of physical barriers or intensive staff supervision. A facility that allows residents access to the community to achieve treatment or correctional objectives, such as through educational or employment programs, typically will not be considered to be a secure juvenile facility.

Security staff means employees primarily responsible for the supervision and control of inmates, detainees, or residents in housing units, recreational areas, dining areas, and other program areas of the facility.

Staff means employees.

Strip search means a search that requires a person to remove or arrange some or all clothing so as to permit a visual inspection of the person’s breasts, buttocks, or genitalia.

Transgender means a person whose gender identity (*i.e.*, internal sense of feeling male or female) is different from the person’s assigned sex at birth.

Substantiated allegation means an allegation that was investigated and determined to have occurred.

Unfounded allegation means an allegation that was investigated and determined not to have occurred.

PREA STANDARDS – FINAL
Adult Prisons and Jails

Unsubstantiated allegation means an allegation that was investigated and the investigation produced insufficient evidence to make a final determination as to whether or not the event occurred.

Volunteer means an individual who donates time and effort on a recurring basis to enhance the activities and programs of the agency.

Youthful inmate means any person under the age of 18 who is under adult court supervision and incarcerated or detained in a prison or jail.

Youthful detainee means any person under the age of 18 who is under adult court supervision and detained in a lockup.

§ 115.6 Definitions related to sexual abuse.

For purposes of this part, the term—

Sexual abuse includes—

- (1) Sexual abuse of an inmate, detainee, or resident by another inmate, detainee, or resident; and
- (2) Sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer.

Sexual abuse of an inmate, detainee, or resident by another inmate, detainee, or resident includes any of the following acts, if the victim does not consent, is coerced into such act by overt or implied threats of violence, or is unable to consent or refuse:

- (1) Contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) Contact between the mouth and the penis, vulva, or anus;
- (3) Penetration of the anal or genital opening of another person, however slight, by a hand, finger, object, or other instrument; and
- (4) Any other intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh, or the buttocks of another person, excluding contact incidental to a physical altercation.

Sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) Contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) Contact between the mouth and the penis, vulva, or anus;
- (3) Contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) Penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) Any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) Any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5) of this section;
- (7) Any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) Voyeurism by a staff member, contractor, or volunteer.

PREA STANDARDS – FINAL
Adult Prisons and Jails

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment includes—

- (1) Repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) Repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

PREA STANDARDS – FINAL
Adult Prisons and Jails

<i>Prevention Planning</i> <i>§ 115.11 Zero tolerance of sexual abuse and sexual harassment; PREA coordinator.</i>
(a) An agency shall have a written policy mandating zero tolerance toward all forms of sexual abuse and sexual harassment and outlining the agency’s approach to preventing, detecting, and responding to such conduct.
(b) An agency shall employ or designate an upper-level, agency-wide PREA coordinator with sufficient time and authority to develop, implement, and oversee agency efforts to comply with the PREA standards in all of its facilities.
(c) Where an agency operates more than one facility, each facility shall designate a PREA compliance manager with sufficient time and authority to coordinate the facility’s efforts to comply with the PREA standards.
<i>Prevention Planning</i> <i>§ 115.12 Contracting with other entities for the confinement of inmates.</i>
(a) A public agency that contracts for the confinement of its inmates with private agencies or other entities, including other government agencies, shall include in any new contract or contract renewal the entity’s obligation to adopt and comply with the PREA standards.
(b) Any new contract or contract renewal shall provide for agency contract monitoring to ensure that the contractor is complying with the PREA standards.
<i>Prevention Planning</i> <i>§ 115.13 Supervision and monitoring.</i>
(a) The agency shall ensure that each facility it operates shall develop, document, and make its best efforts to comply on a regular basis with a staffing plan that provides for adequate levels of staffing, and, where applicable, video monitoring, to protect inmates against sexual abuse. In calculating adequate staffing levels and determining the need for video monitoring, facilities shall take into consideration: <ol style="list-style-type: none"> (1) Generally accepted detention and correctional practices; (2) Any judicial findings of inadequacy; (3) Any findings of inadequacy from Federal investigative agencies; (4) Any findings of inadequacy from internal or external oversight bodies; (5) All components of the facility’s physical plant (including “blind-spots” or areas where staff or inmates may be isolated); (6) The composition of the inmate population; (7) The number and placement of supervisory staff; (8) Institution programs occurring on a particular shift; (9) Any applicable State or local laws, regulations, or standards; (10) The prevalence of substantiated and unsubstantiated incidents of sexual abuse; and (11) Any other relevant factors.
(b) In circumstances where the staffing plan is not complied with, the facility shall document and justify all deviations from the plan.
(c) Whenever necessary, but no less frequently than once each year, for each facility the agency operates, in consultation with the PREA coordinator required by § 115.11, the agency shall assess, determine, and document whether adjustments are needed to: <ol style="list-style-type: none"> (1) The staffing plan established pursuant to paragraph (a) of this section; (2) The facility’s deployment of video monitoring systems and other monitoring technologies; and (3) The resources the facility has available to commit to ensure adherence to the staffing plan.
(d) Each agency operating a facility shall implement a policy and practice of having intermediate-level or higher-level supervisors conduct and document unannounced rounds to identify and deter staff sexual abuse and sexual harassment. Such policy and practice shall be implemented for night shifts as well as day shifts. Each agency shall have a policy to prohibit staff from alerting other staff members that these supervisory rounds are occurring, unless such announcement is related to the legitimate operational functions of the facility.

PREA STANDARDS – FINAL
Adult Prisons and Jails

<i>Prevention Planning</i> <i>§ 115.14 Youthful inmates.</i>
(a) A youthful inmate shall not be placed in a housing unit in which the youthful inmate will have sight, sound, or physical contact with any adult inmate through use of a shared dayroom or other common space, shower area, or sleeping quarters.
(b) In areas outside of housing units, agencies shall either: (1) maintain sight and sound separation between youthful inmates and adult inmates, or (2) provide direct staff supervision when youthful inmates and adult inmates have sight, sound, or physical contact.
(c) Agencies shall make best efforts to avoid placing youthful inmates in isolation to comply with this provision. Absent exigent circumstances, agencies shall not deny youthful inmates daily large-muscle exercise and any legally required special education services to comply with this provision. Youthful inmates shall also have access to other programs and work opportunities to the extent possible.
<i>Prevention Planning</i> <i>§ 115.15 Limits to cross-gender viewing and searches.</i>
(a) The facility shall not conduct cross-gender strip searches or cross-gender visual body cavity searches (meaning a search of the anal or genital opening) except in exigent circumstances or when performed by medical practitioners.
(b) As of [INSERT DATE 3 YEARS PLUS 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], or [INSERT DATE 5 YEARS PLUS 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] for a facility whose rated capacity does not exceed 50 inmates, the facility shall not permit cross-gender pat-down searches of female inmates, absent exigent circumstances. Facilities shall not restrict female inmates' access to regularly available programming or other out-of-cell opportunities in order to comply with this provision.
(c) The facility shall document all cross-gender strip searches and cross-gender visual body cavity searches, and shall document all cross-gender pat-down searches of female inmates.
(d) The facility shall implement policies and procedures that enable inmates to shower, perform bodily functions, and change clothing without nonmedical staff of the opposite gender viewing their breasts, buttocks, or genitalia, except in exigent circumstances or when such viewing is incidental to routine cell checks. Such policies and procedures shall require staff of the opposite gender to announce their presence when entering an inmate housing unit.
(e) The facility shall not search or physically examine a transgender or intersex inmate for the sole purpose of determining the inmate's genital status. If the inmate's genital status is unknown, it may be determined during conversations with the inmate, by reviewing medical records, or, if necessary, by learning that information as part of a broader medical examination conducted in private by a medical practitioner.
(f) The agency shall train security staff in how to conduct cross-gender pat-down searches, and searches of transgender and intersex inmates, in a professional and respectful manner, and in the least intrusive manner possible, consistent with security needs.
<i>Prevention Planning</i> <i>§ 115.16 Inmates with disabilities and inmates who are limited English proficient.</i>
(a) The agency shall take appropriate steps to ensure that inmates with disabilities (including, for example, inmates who are deaf or hard of hearing, those who are blind or have low vision, or those who have intellectual, psychiatric, or speech disabilities), have an equal opportunity to participate in or benefit from all aspects of the agency's efforts to prevent, detect, and respond to sexual abuse and sexual harassment. Such steps shall include, when necessary to ensure effective communication with inmates who are deaf or hard of hearing, providing access to interpreters who can interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary. In addition, the agency shall ensure that written materials are provided in formats or through methods that ensure effective communication with inmates with disabilities, including inmates who have intellectual disabilities, limited reading skills, or who are blind or have low vision. An agency is not required to take actions that it can demonstrate would result in a fundamental alteration in the nature of a service, program, or activity, or in undue financial and administrative burdens, as

PREA STANDARDS – FINAL
Adult Prisons and Jails

those terms are used in regulations promulgated under title II of the Americans With Disabilities Act, 28 CFR 35.164.
(b) The agency shall take reasonable steps to ensure meaningful access to all aspects of the agency’s efforts to prevent, detect, and respond to sexual abuse and sexual harassment to inmates who are limited English proficient, including steps to provide interpreters who can interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary.
(c) The agency shall not rely on inmate interpreters, inmate readers, or other types of inmate assistants except in limited circumstances where an extended delay in obtaining an effective interpreter could compromise the inmate’s safety, the performance of first-response duties under § 115.64, or the investigation of the inmate’s allegations.
<i>Prevention Planning</i> <i>§ 115.17 Hiring and promotion decisions.</i>
(a) The agency shall not hire or promote anyone who may have contact with inmates, and shall not enlist the services of any contractor who may have contact with inmates, who— (1) Has engaged in sexual abuse in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution (as defined in 42 U.S.C. 1997); (2) Has been convicted of engaging or attempting to engage in sexual activity in the community facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse; or (3) Has been civilly or administratively adjudicated to have engaged in the activity described in paragraph (a)(2) of this section.
(b) The agency shall consider any incidents of sexual harassment in determining whether to hire or promote anyone, or to enlist the services of any contractor, who may have contact with inmates.
(c) Before hiring new employees who may have contact with inmates, the agency shall: (1) Perform a criminal background records check; and (2) Consistent with Federal, State, and local law, make its best efforts to contact all prior institutional employers for information on substantiated allegations of sexual abuse or any resignation during a pending investigation of an allegation of sexual abuse.
(d) The agency shall also perform a criminal background records check before enlisting the services of any contractor who may have contact with inmates.
(e) The agency shall either conduct criminal background records checks at least every five years of current employees and contractors who may have contact with inmates or have in place a system for otherwise capturing such information for current employees.
(f) The agency shall ask all applicants and employees who may have contact with inmates directly about previous misconduct described in paragraph (a) of this section in written applications or interviews for hiring or promotions and in any interviews or written self-evaluations conducted as part of reviews of current employees. The agency shall also impose upon employees a continuing affirmative duty to disclose any such misconduct.
(g) Material omissions regarding such misconduct, or the provision of materially false information, shall be grounds for termination.
(h) Unless prohibited by law, the agency shall provide information on substantiated allegations of sexual abuse or sexual harassment involving a former employee upon receiving a request from an institutional employer for whom such employee has applied to work.
<i>Prevention Planning</i> <i>§ 115.18 Upgrades to facilities and technologies.</i>
(a) When designing or acquiring any new facility and in planning any substantial expansion or modification of existing facilities, the agency shall consider the effect of the design, acquisition, expansion, or modification upon the agency’s ability to protect inmates from sexual abuse.
(b) When installing or updating a video monitoring system, electronic surveillance system, or other monitoring technology, the agency shall consider how such technology may enhance the agency’s ability to protect inmates from sexual abuse.
<i>Responsive Planning</i>

PREA STANDARDS – FINAL
Adult Prisons and Jails

<i>§ 115.21 Evidence protocol and forensic medical examinations.</i>
(a) To the extent the agency is responsible for investigating allegations of sexual abuse, the agency shall follow a uniform evidence protocol that maximizes the potential for obtaining usable physical evidence for administrative proceedings and criminal prosecutions.
(b) The protocol shall be developmentally appropriate for youth where applicable, and, as appropriate, shall be adapted from or otherwise based on the most recent edition of the U.S. Department of Justice’s Office on Violence Against Women publication, “A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents,” or similarly comprehensive and authoritative protocols developed after 2011.
(c) The agency shall offer all victims of sexual abuse access to forensic medical examinations, whether on-site or at an outside facility, without financial cost, where evidentiarily or medically appropriate. Such examinations shall be performed by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs) where possible. If SAFEs or SANEs cannot be made available, the examination can be performed by other qualified medical practitioners. The agency shall document its efforts to provide SAFEs or SANEs.
(d) The agency shall attempt to make available to the victim a victim advocate from a rape crisis center. If a rape crisis center is not available to provide victim advocate services, the agency shall make available to provide these services a qualified staff member from a community-based organization, or a qualified agency staff member. Agencies shall document efforts to secure services from rape crisis centers. For the purpose of this standard, a rape crisis center refers to an entity that provides intervention and related assistance, such as the services specified in 42 U.S.C. 14043g(b)(2)(C), to victims of sexual assault of all ages. The agency may utilize a rape crisis center that is part of a governmental unit as long as the center is not part of the criminal justice system (such as a law enforcement agency) and offers a comparable level of confidentiality as a nongovernmental entity that provides similar victim services.
(e) As requested by the victim, the victim advocate, qualified agency staff member, or qualified community-based organization staff member shall accompany and support the victim through the forensic medical examination process and investigatory interviews and shall provide emotional support, crisis intervention, information, and referrals.
(f) To the extent the agency itself is not responsible for investigating allegations of sexual abuse, the agency shall request that the investigating agency follow the requirements of paragraphs (a) through (e) of this section.
(g) The requirements of paragraphs (a) through (f) of this section shall also apply to: (1) Any State entity outside of the agency that is responsible for investigating allegations of sexual abuse in prisons or jails; and (2) Any Department of Justice component that is responsible for investigating allegations of sexual abuse in prisons or jails.
(h) For the purposes of this section, a qualified agency staff member or a qualified community-based staff member shall be an individual who has been screened for appropriateness to serve in this role and has received education concerning sexual assault and forensic examination issues in general.
<i>Responsive Planning</i>
<i>§ 115.22 Policies to ensure referrals of allegations for investigations.</i>
(a) The agency shall ensure that an administrative or criminal investigation is completed for all allegations of sexual abuse and sexual harassment.
(b) The agency shall have in place a policy to ensure that allegations of sexual abuse or sexual harassment are referred for investigation to an agency with the legal authority to conduct criminal investigations, unless the allegation does not involve potentially criminal behavior. The agency shall publish such policy on its website or, if it does not have one, make the policy available through other means. The agency shall document all such referrals.
(c) If a separate entity is responsible for conducting criminal investigations, such publication shall describe the responsibilities of both the agency and the investigating entity.
(d) Any State entity responsible for conducting administrative or criminal investigations of sexual abuse or sexual harassment in prisons or jails shall have in place a policy governing the conduct of such investigations.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(e) Any Department of Justice component responsible for conducting administrative or criminal investigations of sexual abuse or sexual harassment in prisons or jails shall have in place a policy governing the conduct of such investigations.

Training and Education
§ 115.31 Employee training.

(a) The agency shall train all employees who may have contact with inmates on:

- (1) Its zero-tolerance policy for sexual abuse and sexual harassment;
- (2) How to fulfill their responsibilities under agency sexual abuse and sexual harassment prevention, detection, reporting, and response policies and procedures;
- (3) Inmates’ right to be free from sexual abuse and sexual harassment;
- (4) The right of inmates and employees to be free from retaliation for reporting sexual abuse and sexual harassment;
- (5) The dynamics of sexual abuse and sexual harassment in confinement;
- (6) The common reactions of sexual abuse and sexual harassment victims;
- (7) How to detect and respond to signs of threatened and actual sexual abuse;
- (8) How to avoid inappropriate relationships with inmates;
- (9) How to communicate effectively and professionally with inmates, including lesbian, gay, bisexual, transgender, intersex, or gender nonconforming inmates; and
- (10) How to comply with relevant laws related to mandatory reporting of sexual abuse to outside authorities.

(b) Such training shall be tailored to the gender of the inmates at the employee’s facility. The employee shall receive additional training if the employee is reassigned from a facility that houses only male inmates to a facility that houses only female inmates, or vice versa.

(c) All current employees who have not received such training shall be trained within one year of the effective date of the PREA standards, and the agency shall provide each employee with refresher training every two years to ensure that all employees know the agency’s current sexual abuse and sexual harassment policies and procedures. In years in which an employee does not receive refresher training, the agency shall provide refresher information on current sexual abuse and sexual harassment policies.

(d) The agency shall document, through employee signature or electronic verification, that employees understand the training they have received.

Training and Education
§ 115.32 Volunteer and contractor training.

(a) The agency shall ensure that all volunteers and contractors who have contact with inmates have been trained on their responsibilities under the agency’s sexual abuse and sexual harassment prevention, detection, and response policies and procedures.

(b) The level and type of training provided to volunteers and contractors shall be based on the services they provide and level of contact they have with inmates, but all volunteers and contractors who have contact with inmates shall be notified of the agency’s zero-tolerance policy regarding sexual abuse and sexual harassment and informed how to report such incidents.

(c) The agency shall maintain documentation confirming that volunteers and contractors understand the training they have received.

Training and Education
§ 115.33 Inmate education.

(a) During the intake process, inmates shall receive information explaining the agency’s zero-tolerance policy regarding sexual abuse and sexual harassment and how to report incidents or suspicions of sexual abuse or sexual harassment.

(b) Within 30 days of intake, the agency shall provide comprehensive education to inmates either in person or through video regarding their rights to be free from sexual abuse and sexual harassment and to be free from retaliation for reporting such incidents, and regarding agency policies and procedures for responding to such incidents.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(c) Current inmates who have not received such education shall be educated within one year of the effective date of the PREA standards, and shall receive education upon transfer to a different facility to the extent that the policies and procedures of the inmate’s new facility differ from those of the previous facility.

(d) The agency shall provide inmate education in formats accessible to all inmates, including those who are limited English proficient, deaf, visually impaired, or otherwise disabled, as well as to inmates who have limited reading skills.

(e) The agency shall maintain documentation of inmate participation in these education sessions.

(f) In addition to providing such education, the agency shall ensure that key information is continuously and readily available or visible to inmates through posters, inmate handbooks, or other written formats.

Training and Education
§ 115.34 Specialized training: Investigations.

(a) In addition to the general training provided to all employees pursuant to § 115.31, the agency shall ensure that, to the extent the agency itself conducts sexual abuse investigations, its investigators have received training in conducting such investigations in confinement settings.

(b) Specialized training shall include techniques for interviewing sexual abuse victims, proper use of Miranda and Garrity warnings, sexual abuse evidence collection in confinement settings, and the criteria and evidence required to substantiate a case for administrative action or prosecution referral.

(c) The agency shall maintain documentation that agency investigators have completed the required specialized training in conducting sexual abuse investigations.

(d) Any State entity or Department of Justice component that investigates sexual abuse in confinement settings shall provide such training to its agents and investigators who conduct such investigations.

Training and Education
§ 115.35 Specialized training: Medical and mental health care.

(a) The agency shall ensure that all full- and part-time medical and mental health care practitioners who work regularly in its facilities have been trained in:

- (1) How to detect and assess signs of sexual abuse and sexual harassment;
- (2) How to preserve physical evidence of sexual abuse;
- (3) How to respond effectively and professionally to victims of sexual abuse and sexual harassment; and
- (4) How and to whom to report allegations or suspicions of sexual abuse and sexual harassment.

(b) If medical staff employed by the agency conduct forensic examinations, such medical staff shall receive the appropriate training to conduct such examinations.

(c) The agency shall maintain documentation that medical and mental health practitioners have received the training referenced in this standard either from the agency or elsewhere.

(d) Medical and mental health care practitioners shall also receive the training mandated for employees under § 115.31 or for contractors and volunteers under § 115.32, depending upon the practitioner’s status at the agency.

Screening for Risk of Sexual Victimization and Abusiveness
§ 115.41 Screening for risk of victimization and abusiveness.

(a) All inmates shall be assessed during an intake screening and upon transfer to another facility for their risk of being sexually abused by other inmates or sexually abusive toward other inmates.

(b) Intake screening shall ordinarily take place within 72 hours of arrival at the facility.

(c) Such assessments shall be conducted using an objective screening instrument.

(d) The intake screening shall consider, at a minimum, the following criteria to assess inmates for risk of sexual victimization:

- (1) Whether the inmate has a mental, physical, or developmental disability;
- (2) The age of the inmate;
- (3) The physical build of the inmate;
- (4) Whether the inmate has previously been incarcerated;
- (5) Whether the inmate’s criminal history is exclusively nonviolent;
- (6) Whether the inmate has prior convictions for sex offenses against an adult or child;
- (7) Whether the inmate is or is perceived to be gay, lesbian, bisexual, transgender, intersex, or gender nonconforming;

PREA STANDARDS – FINAL
Adult Prisons and Jails

<p>(8) Whether the inmate has previously experienced sexual victimization;</p> <p>(9) The inmate’s own perception of vulnerability; and</p> <p>(10) Whether the inmate is detained solely for civil immigration purposes.</p>
<p>(e) The initial screening shall consider prior acts of sexual abuse, prior convictions for violent offenses, and history of prior institutional violence or sexual abuse, as known to the agency, in assessing inmates for risk of being sexually abusive.</p>
<p>(f) Within a set time period, not to exceed 30 days from the inmate’s arrival at the facility, the facility will reassess the inmate’s risk of victimization or abusiveness based upon any additional, relevant information received by the facility since the intake screening.</p>
<p>(g) An inmate’s risk level shall be reassessed when warranted due to a referral, request, incident of sexual abuse, or receipt of additional information that bears on the inmate’s risk of sexual victimization or abusiveness.</p>
<p>(h) Inmates may not be disciplined for refusing to answer, or for not disclosing complete information in response to, questions asked pursuant to paragraphs (d)(1), (d)(7), (d)(8), or (d)(9) of this section.</p>
<p>(i) The agency shall implement appropriate controls on the dissemination within the facility of responses to questions asked pursuant to this standard in order to ensure that sensitive information is not exploited to the inmate’s detriment by staff or other inmates.</p>
<p><i>Screening for Risk of Sexual Victimization and Abusiveness</i> <i>§ 115.42 Use of screening information.</i></p>
<p>(a) The agency shall use information from the risk screening required by § 115.41 to inform housing, bed, work, education, and program assignments with the goal of keeping separate those inmates at high risk of being sexually victimized from those at high risk of being sexually abusive.</p>
<p>(b) The agency shall make individualized determinations about how to ensure the safety of each inmate.</p>
<p>(c) In deciding whether to assign a transgender or intersex inmate to a facility for male or female inmates, and in making other housing and programming assignments, the agency shall consider on a case-by-case basis whether a placement would ensure the inmate’s health and safety, and whether the placement would present management or security problems.</p>
<p>(d) Placement and programming assignments for each transgender or intersex inmate shall be reassessed at least twice each year to review any threats to safety experienced by the inmate.</p>
<p>(e) A transgender or intersex inmate’s own views with respect to his or her own safety shall be given serious consideration.</p>
<p>(f) Transgender and intersex inmates shall be given the opportunity to shower separately from other inmates.</p>
<p>(g) The agency shall not place lesbian, gay, bisexual, transgender, or intersex inmates in dedicated facilities, units, or wings solely on the basis of such identification or status, unless such placement is in a dedicated facility, unit, or wing established in connection with a consent decree, legal settlement, or legal judgment for the purpose of protecting such inmates.</p>
<p><i>Screening for Risk of Sexual Victimization and Abusiveness</i> <i>§ 115.43 Protective custody.</i></p>
<p>(a) Inmates at high risk for sexual victimization shall not be placed in involuntary segregated housing unless an assessment of all available alternatives has been made, and a determination has been made that there is no available alternative means of separation from likely abusers. If a facility cannot conduct such an assessment immediately, the facility may hold the inmate in involuntary segregated housing for less than 24 hours while completing the assessment.</p>
<p>(b) Inmates placed in segregated housing for this purpose shall have access to programs, privileges, education, and work opportunities to the extent possible. If the facility restricts access to programs, privileges, education, or work opportunities, the facility shall document:</p> <ol style="list-style-type: none"> (1) The opportunities that have been limited; (2) The duration of the limitation; and (3) The reasons for such limitations.
<p>(c) The facility shall assign such inmates to involuntary segregated housing only until an alternative means of separation from likely abusers can be arranged, and such an assignment shall not ordinarily exceed a period of 30 days.</p>

PREA STANDARDS – FINAL
Adult Prisons and Jails

(d) If an involuntary segregated housing assignment is made pursuant to paragraph (a) of this section, the facility shall clearly document:

- (1) The basis for the facility's concern for the inmate's safety; and
- (2) The reason why no alternative means of separation can be arranged.

(e) Every 30 days, the facility shall afford each such inmate a review to determine whether there is a continuing need for separation from the general population.

PREA STANDARDS – FINAL
Adult Prisons and Jails

<i>Reporting</i> <i>§ 115.51 Inmate reporting.</i>
(a) The agency shall provide multiple internal ways for inmates to privately report sexual abuse and sexual harassment, retaliation by other inmates or staff for reporting sexual abuse and sexual harassment, and staff neglect or violation of responsibilities that may have contributed to such incidents.
(b) The agency shall also provide at least one way for inmates to report abuse or harassment to a public or private entity or office that is not part of the agency, and that is able to receive and immediately forward inmate reports of sexual abuse and sexual harassment to agency officials, allowing the inmate to remain anonymous upon request. Inmates detained solely for civil immigration purposes shall be provided information on how to contact relevant consular officials and relevant officials at the Department of Homeland Security.
(c) Staff shall accept reports made verbally, in writing, anonymously, and from third parties and shall promptly document any verbal reports.
(d) The agency shall provide a method for staff to privately report sexual abuse and sexual harassment of inmates.
<i>Reporting</i> <i>§ 115.52 Exhaustion of administrative remedies.</i>
(a) An agency shall be exempt from this standard if it does not have administrative procedures to address inmate grievances regarding sexual abuse.
(b)(1) The agency shall not impose a time limit on when an inmate may submit a grievance regarding an allegation of sexual abuse. (2) The agency may apply otherwise-applicable time limits to any portion of a grievance that does not allege an incident of sexual abuse. (3) The agency shall not require an inmate to use any informal grievance process, or to otherwise attempt to resolve with staff, an alleged incident of sexual abuse. (4) Nothing in this section shall restrict the agency’s ability to defend against an inmate lawsuit on the ground that the applicable statute of limitations has expired.
(c) The agency shall ensure that— (1) An inmate who alleges sexual abuse may submit a grievance without submitting it to a staff member who is the subject of the complaint, and (2) Such grievance is not referred to a staff member who is the subject of the complaint.
(d)(1) The agency shall issue a final agency decision on the merits of any portion of a grievance alleging sexual abuse within 90 days of the initial filing of the grievance. (2) Computation of the 90-day time period shall not include time consumed by inmates in preparing any administrative appeal. (3) The agency may claim an extension of time to respond, of up to 70 days, if the normal time period for response is insufficient to make an appropriate decision. The agency shall notify the inmate in writing of any such extension and provide a date by which a decision will be made. (4) At any level of the administrative process, including the final level, if the inmate does not receive a response within the time allotted for reply, including any properly noticed extension, the inmate may consider the absence of a response to be a denial at that level.
(e)(1) Third parties, including fellow inmates, staff members, family members, attorneys, and outside advocates, shall be permitted to assist inmates in filing requests for administrative remedies relating to allegations of sexual abuse, and shall also be permitted to file such requests on behalf of inmates. (2) If a third party files such a request on behalf of an inmate, the facility may require as a condition of processing the request that the alleged victim agree to have the request filed on his or her behalf, and may also require the alleged victim to personally pursue any subsequent steps in the administrative remedy process. (3) If the inmate declines to have the request processed on his or her behalf, the agency shall document the inmate’s decision.
(f)(1) The agency shall establish procedures for the filing of an emergency grievance alleging that an inmate is subject to a substantial risk of imminent sexual abuse.

PREA STANDARDS – FINAL
Adult Prisons and Jails

<p>(2) After receiving an emergency grievance alleging an inmate is subject to a substantial risk of imminent sexual abuse, the agency shall immediately forward the grievance (or any portion thereof that alleges the substantial risk of imminent sexual abuse) to a level of review at which immediate corrective action may be taken, shall provide an initial response within 48 hours, and shall issue a final agency decision within 5 calendar days. The initial response and final agency decision shall document the agency’s determination whether the inmate is in substantial risk of imminent sexual abuse and the action taken in response to the emergency grievance.</p>
<p>(g) The agency may discipline an inmate for filing a grievance related to alleged sexual abuse only where the agency demonstrates that the inmate filed the grievance in bad faith.</p>
<p><i>Reporting</i> <i>§ 115.53 Inmate access to outside confidential support services.</i></p>
<p>(a) The facility shall provide inmates with access to outside victim advocates for emotional support services related to sexual abuse by giving inmates mailing addresses and telephone numbers, including toll-free hotline numbers where available, of local, State, or national victim advocacy or rape crisis organizations, and, for persons detained solely for civil immigration purposes, immigrant services agencies. The facility shall enable reasonable communication between inmates and these organizations and agencies, in as confidential a manner as possible.</p>
<p>(b) The facility shall inform inmates, prior to giving them access, of the extent to which such communications will be monitored and the extent to which reports of abuse will be forwarded to authorities in accordance with mandatory reporting laws.</p>
<p>(c) The agency shall maintain or attempt to enter into memoranda of understanding or other agreements with community service providers that are able to provide inmates with confidential emotional support services related to sexual abuse. The agency shall maintain copies of agreements or documentation showing attempts to enter into such agreements.</p>
<p><i>Reporting</i> <i>§ 115.54 Third-party reporting.</i></p>
<p>The agency shall establish a method to receive third-party reports of sexual abuse and sexual harassment and shall distribute publicly information on how to report sexual abuse and sexual harassment on behalf of an inmate.</p>
<p><i>Official Response Following an Inmate Report</i> <i>§ 115.61 Staff and agency reporting duties.</i></p>
<p>(a) The agency shall require all staff to report immediately and according to agency policy any knowledge, suspicion, or information regarding an incident of sexual abuse or sexual harassment that occurred in a facility, whether or not it is part of the agency; retaliation against inmates or staff who reported such an incident; and any staff neglect or violation of responsibilities that may have contributed to an incident or retaliation.</p>
<p>(b) Apart from reporting to designated supervisors or officials, staff shall not reveal any information related to a sexual abuse report to anyone other than to the extent necessary, as specified in agency policy, to make treatment, investigation, and other security and management decisions.</p>
<p>(c) Unless otherwise precluded by Federal, State, or local law, medical and mental health practitioners shall be required to report sexual abuse pursuant to paragraph (a) of this section and to inform inmates of the practitioner’s duty to report, and the limitations of confidentiality, at the initiation of services.</p>
<p>(d) If the alleged victim is under the age of 18 or considered a vulnerable adult under a State or local vulnerable persons statute, the agency shall report the allegation to the designated State or local services agency under applicable mandatory reporting laws.</p>
<p>(e) The facility shall report all allegations of sexual abuse and sexual harassment, including third-party and anonymous reports, to the facility’s designated investigators.</p>
<p><i>Official Response Following an Inmate Report</i> <i>§ 115.62 Agency protection duties.</i></p>
<p>When an agency learns that an inmate is subject to a substantial risk of imminent sexual abuse, it shall take immediate action to protect the inmate.</p>
<p><i>Official Response Following an Inmate Report</i> <i>§ 115.63 Reporting to other confinement facilities.</i></p>

PREA STANDARDS – FINAL
Adult Prisons and Jails

(a) Upon receiving an allegation that an inmate was sexually abused while confined at another facility, the head of the facility that received the allegation shall notify the head of the facility or appropriate office of the agency where the alleged abuse occurred.
(b) Such notification shall be provided as soon as possible, but no later than 72 hours after receiving the allegation.
(c) The agency shall document that it has provided such notification.
(d) The facility head or agency office that receives such notification shall ensure that the allegation is investigated in accordance with these standards.
<i>Official Response Following an Inmate Report</i> <i>§ 115.64 Staff first responder duties.</i>
(a) Upon learning of an allegation that an inmate was sexually abused, the first security staff member to respond to the report shall be required to:
(1) Separate the alleged victim and abuser;
(2) Preserve and protect any crime scene until appropriate steps can be taken to collect any evidence;
(3) If the abuse occurred within a time period that still allows for the collection of physical evidence, request that the alleged victim not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking, or eating; and
(4) If the abuse occurred within a time period that still allows for the collection of physical evidence, ensure that the alleged abuser does not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking, or eating.
(b) If the first staff responder is not a security staff member, the responder shall be required to request that the alleged victim not take any actions that could destroy physical evidence, and then notify security staff.
<i>Official Response Following an Inmate Report</i> <i>§ 115.65 Coordinated response.</i>
The facility shall develop a written institutional plan to coordinate actions taken in response to an incident of sexual abuse, among staff first responders, medical and mental health practitioners, investigators, and facility leadership.
<i>Official Response Following an Inmate Report</i> <i>§ 115.66 Preservation of ability to protect inmates from contact with abusers.</i>
(a) Neither the agency nor any other governmental entity responsible for collective bargaining on the agency’s behalf shall enter into or renew any collective bargaining agreement or other agreement that limits the agency’s ability to remove alleged staff sexual abusers from contact with any inmates pending the outcome of an investigation or of a determination of whether and to what extent discipline is warranted.
(b) Nothing in this standard shall restrict the entering into or renewal of agreements that govern:
(1) The conduct of the disciplinary process, as long as such agreements are not inconsistent with the provisions of §§ 115.72 and 115.76; or
(2) Whether a no-contact assignment that is imposed pending the outcome of an investigation shall be expunged from or retained in the staff member’s personnel file following a determination that the allegation of sexual abuse is not substantiated.
<i>Official Response Following an Inmate Report</i> <i>§ 115.67 Agency protection against retaliation.</i>
(a) The agency shall establish a policy to protect all inmates and staff who report sexual abuse or sexual harassment or cooperate with sexual abuse or sexual harassment investigations from retaliation by other inmates or staff, and shall designate which staff members or departments are charged with monitoring retaliation.
(b) The agency shall employ multiple protection measures, such as housing changes or transfers for inmate victims or abusers, removal of alleged staff or inmate abusers from contact with victims, and emotional support services for inmates or staff who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations.
(c) For at least 90 days following a report of sexual abuse, the agency shall monitor the conduct and treatment of inmates or staff who reported the sexual abuse and of inmates who were reported to have suffered sexual abuse to see if there are changes that may suggest possible retaliation by inmates or staff, and shall act promptly to

PREA STANDARDS – FINAL
Adult Prisons and Jails

remedy any such retaliation. Items the agency should monitor include any inmate disciplinary reports, housing, or program changes, or negative performance reviews or reassignments of staff. The agency shall continue such monitoring beyond 90 days if the initial monitoring indicates a continuing need.
(d) In the case of inmates, such monitoring shall also include periodic status checks.
(e) If any other individual who cooperates with an investigation expresses a fear of retaliation, the agency shall take appropriate measures to protect that individual against retaliation.
(f) An agency’s obligation to monitor shall terminate if the agency determines that the allegation is unfounded.
<i>Official Response Following an Inmate Report</i> <i>§ 115.68 Post-allegation protective custody.</i>
Any use of segregated housing to protect an inmate who is alleged to have suffered sexual abuse shall be subject to the requirements of § 115.43.
<i>Investigations</i> <i>§ 115.71 Criminal and administrative agency investigations.</i>
(a) When the agency conducts its own investigations into allegations of sexual abuse and sexual harassment, it shall do so promptly, thoroughly, and objectively for all allegations, including third-party and anonymous reports.
(b) Where sexual abuse is alleged, the agency shall use investigators who have received special training in sexual abuse investigations pursuant to § 115.34.
(c) Investigators shall gather and preserve direct and circumstantial evidence, including any available physical and DNA evidence and any available electronic monitoring data; shall interview alleged victims, suspected perpetrators, and witnesses; and shall review prior complaints and reports of sexual abuse involving the suspected perpetrator.
(d) When the quality of evidence appears to support criminal prosecution, the agency shall conduct compelled interviews only after consulting with prosecutors as to whether compelled interviews may be an obstacle for subsequent criminal prosecution.
(e) The credibility of an alleged victim, suspect, or witness shall be assessed on an individual basis and shall not be determined by the person’s status as inmate or staff. No agency shall require an inmate who alleges sexual abuse to submit to a polygraph examination or other truth-telling device as a condition for proceeding with the investigation of such an allegation.
(f) Administrative investigations: (1) Shall include an effort to determine whether staff actions or failures to act contributed to the abuse; and (2) Shall be documented in written reports that include a description of the physical and testimonial evidence, the reasoning behind credibility assessments, and investigative facts and findings.
(g) Criminal investigations shall be documented in a written report that contains a thorough description of physical, testimonial, and documentary evidence and attaches copies of all documentary evidence where feasible.
(h) Substantiated allegations of conduct that appears to be criminal shall be referred for prosecution.
(i) The agency shall retain all written reports referenced in paragraphs (f) and (g) of this section for as long as the alleged abuser is incarcerated or employed by the agency, plus five years.
(j) The departure of the alleged abuser or victim from the employment or control of the facility or agency shall not provide a basis for terminating an investigation.
(k) Any State entity or Department of Justice component that conducts such investigations shall do so pursuant to the above requirements.
(l) When outside agencies investigate sexual abuse, the facility shall cooperate with outside investigators and shall endeavor to remain informed about the progress of the investigation.
<i>Investigations</i> <i>§ 115.72 Evidentiary standard for administrative investigations.</i>
The agency shall impose no standard higher than a preponderance of the evidence in determining whether allegations of sexual abuse or sexual harassment are substantiated.
<i>Investigations</i> <i>§ 115.73 Reporting to inmates.</i>

PREA STANDARDS – FINAL
Adult Prisons and Jails

- (a) Following an investigation into an inmate’s allegation that he or she suffered sexual abuse in an agency facility, the agency shall inform the inmate as to whether the allegation has been determined to be substantiated, unsubstantiated, or unfounded.
- (b) If the agency did not conduct the investigation, it shall request the relevant information from the investigative agency in order to inform the inmate.
- (c) Following an inmate’s allegation that a staff member has committed sexual abuse against the inmate, the agency shall subsequently inform the inmate (unless the agency has determined that the allegation is unfounded) whenever:
- (1) The staff member is no longer posted within the inmate’s unit;
 - (2) The staff member is no longer employed at the facility;
 - (3) The agency learns that the staff member has been indicted on a charge related to sexual abuse within the facility; or
 - (4) The agency learns that the staff member has been convicted on a charge related to sexual abuse within the facility.
- (d) Following an inmate’s allegation that he or she has been sexually abused by another inmate, the agency shall subsequently inform the alleged victim whenever:
- (1) The agency learns that the alleged abuser has been indicted on a charge related to sexual abuse within the facility; or
 - (2) The agency learns that the alleged abuser has been convicted on a charge related to sexual abuse within the facility.
- (e) All such notifications or attempted notifications shall be documented.
- (f) An agency’s obligation to report under this standard shall terminate if the inmate is released from the agency’s custody.

Discipline
§ 115.76 Disciplinary sanctions for staff.

- (a) Staff shall be subject to disciplinary sanctions up to and including termination for violating agency sexual abuse or sexual harassment policies.
- (b) Termination shall be the presumptive disciplinary sanction for staff who have engaged in sexual abuse.
- (c) Disciplinary sanctions for violations of agency policies relating to sexual abuse or sexual harassment (other than actually engaging in sexual abuse) shall be commensurate with the nature and circumstances of the acts committed, the staff member’s disciplinary history, and the sanctions imposed for comparable offenses by other staff with similar histories.
- (d) All terminations for violations of agency sexual abuse or sexual harassment policies, or resignations by staff who would have been terminated if not for their resignation, shall be reported to law enforcement agencies, unless the activity was clearly not criminal, and to any relevant licensing bodies.

Discipline
§ 115.77 Corrective action for contractors and volunteers.

- (a) Any contractor or volunteer who engages in sexual abuse shall be prohibited from contact with inmates and shall be reported to law enforcement agencies, unless the activity was clearly not criminal, and to relevant licensing bodies.
- (b) The facility shall take appropriate remedial measures, and shall consider whether to prohibit further contact with inmates, in the case of any other violation of agency sexual abuse or sexual harassment policies by a contractor or volunteer.

Discipline
§ 115.78 Disciplinary sanctions for inmates.

- (a) Inmates shall be subject to disciplinary sanctions pursuant to a formal disciplinary process following an administrative finding that the inmate engaged in inmate-on-inmate sexual abuse or following a criminal finding of guilt for inmate-on-inmate sexual abuse.
- (b) Sanctions shall be commensurate with the nature and circumstances of the abuse committed, the inmate’s disciplinary history, and the sanctions imposed for comparable offenses by other inmates with similar histories.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(c) The disciplinary process shall consider whether an inmate’s mental disabilities or mental illness contributed to his or her behavior when determining what type of sanction, if any, should be imposed.
(d) If the facility offers therapy, counseling, or other interventions designed to address and correct underlying reasons or motivations for the abuse, the facility shall consider whether to require the offending inmate to participate in such interventions as a condition of access to programming or other benefits.
(e) The agency may discipline an inmate for sexual contact with staff only upon a finding that the staff member did not consent to such contact.
(f) For the purpose of disciplinary action, a report of sexual abuse made in good faith based upon a reasonable belief that the alleged conduct occurred shall not constitute falsely reporting an incident or lying, even if an investigation does not establish evidence sufficient to substantiate the allegation.
(g) An agency may, in its discretion, prohibit all sexual activity between inmates and may discipline inmates for such activity. An agency may not, however, deem such activity to constitute sexual abuse if it determines that the activity is not coerced.
<i>Medical and Mental Care</i> <i>§ 115.81 Medical and mental health screenings; history of sexual abuse.</i>
(a) If the screening pursuant to § 115.41 indicates that a prison inmate has experienced prior sexual victimization, whether it occurred in an institutional setting or in the community, staff shall ensure that the inmate is offered a follow-up meeting with a medical or mental health practitioner within 14 days of the intake screening.
(b) If the screening pursuant to § 115.41 indicates that a prison inmate has previously perpetrated sexual abuse, whether it occurred in an institutional setting or in the community, staff shall ensure that the inmate is offered a follow-up meeting with a mental health practitioner within 14 days of the intake screening.
(c) If the screening pursuant to § 115.41 indicates that a jail inmate has experienced prior sexual victimization, whether it occurred in an institutional setting or in the community, staff shall ensure that the inmate is offered a follow-up meeting with a medical or mental health practitioner within 14 days of the intake screening.
(d) Any information related to sexual victimization or abusiveness that occurred in an institutional setting shall be strictly limited to medical and mental health practitioners and other staff, as necessary, to inform treatment plans and security and management decisions, including housing, bed, work, education, and program assignments, or as otherwise required by Federal, State, or local law.
(e) Medical and mental health practitioners shall obtain informed consent from inmates before reporting information about prior sexual victimization that did not occur in an institutional setting, unless the inmate is under the age of 18.
<i>Medical and Mental Care</i> <i>§ 115.82 Access to emergency medical and mental health services.</i>
(a) Inmate victims of sexual abuse shall receive timely, unimpeded access to emergency medical treatment and crisis intervention services, the nature and scope of which are determined by medical and mental health practitioners according to their professional judgment.
(b) If no qualified medical or mental health practitioners are on duty at the time a report of recent abuse is made, security staff first responders shall take preliminary steps to protect the victim pursuant to § 115.62 and shall immediately notify the appropriate medical and mental health practitioners.
(c) Inmate victims of sexual abuse while incarcerated shall be offered timely information about and timely access to emergency contraception and sexually transmitted infections prophylaxis, in accordance with professionally accepted standards of care, where medically appropriate.
(d) Treatment services shall be provided to the victim without financial cost and regardless of whether the victim names the abuser or cooperates with any investigation arising out of the incident.
<i>Medical and Mental Care</i> <i>§ 115.83 Ongoing medical and mental health care for sexual abuse victims and abusers.</i>
(a) The facility shall offer medical and mental health evaluation and, as appropriate, treatment to all inmates who have been victimized by sexual abuse in any prison, jail, lockup, or juvenile facility.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(b) The evaluation and treatment of such victims shall include, as appropriate, follow-up services, treatment plans, and, when necessary, referrals for continued care following their transfer to, or placement in, other facilities, or their release from custody.
(c) The facility shall provide such victims with medical and mental health services consistent with the community level of care.
(d) Inmate victims of sexually abusive vaginal penetration while incarcerated shall be offered pregnancy tests.
(e) If pregnancy results from the conduct described in paragraph (d) of this section, such victims shall receive timely and comprehensive information about and timely access to all lawful pregnancy-related medical services.
(f) Inmate victims of sexual abuse while incarcerated shall be offered tests for sexually transmitted infections as medically appropriate.
(g) Treatment services shall be provided to the victim without financial cost and regardless of whether the victim names the abuser or cooperates with any investigation arising out of the incident.
(h) All prisons shall attempt to conduct a mental health evaluation of all known inmate-on-inmate abusers within 60 days of learning of such abuse history and offer treatment when deemed appropriate by mental health practitioners.
<i>Data Collection and Review</i> <i>§ 115.86 Sexual abuse incident reviews.</i>
(a) The facility shall conduct a sexual abuse incident review at the conclusion of every sexual abuse investigation, including where the allegation has not been substantiated, unless the allegation has been determined to be unfounded.
(b) Such review shall ordinarily occur within 30 days of the conclusion of the investigation.
(c) The review team shall include upper-level management officials, with input from line supervisors, investigators, and medical or mental health practitioners.
(d) The review team shall: <ul style="list-style-type: none"> (1) Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect, or respond to sexual abuse; (2) Consider whether the incident or allegation was motivated by race; ethnicity; gender identity; lesbian, gay, bisexual, transgender, or intersex identification, status, or perceived status; or gang affiliation; or was motivated or otherwise caused by other group dynamics at the facility; (3) Examine the area in the facility where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse; (4) Assess the adequacy of staffing levels in that area during different shifts; (5) Assess whether monitoring technology should be deployed or augmented to supplement supervision by staff; and (6) Prepare a report of its findings, including but not necessarily limited to determinations made pursuant to paragraphs (d)(1)-(d)(5) of this section, and any recommendations for improvement and submit such report to the facility head and PREA compliance manager.
(e) The facility shall implement the recommendations for improvement, or shall document its reasons for not doing so.
<i>Data Collection and Review</i> <i>§ 115.87 Data collection.</i>
(a) The agency shall collect accurate, uniform data for every allegation of sexual abuse at facilities under its direct control using a standardized instrument and set of definitions.
(b) The agency shall aggregate the incident-based sexual abuse data at least annually.
(c) The incident-based data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the Survey of Sexual Violence conducted by the Department of Justice.
(d) The agency shall maintain, review, and collect data as needed from all available incident-based documents, including reports, investigation files, and sexual abuse incident reviews.
(e) The agency also shall obtain incident-based and aggregated data from every private facility with which it contracts for the confinement of its inmates.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(f) Upon request, the agency shall provide all such data from the previous calendar year to the Department of Justice no later than June 30.
<i>Data Collection and Review</i> <i>§ 115.88 Data review for corrective action.</i>
(a) The agency shall review data collected and aggregated pursuant to § 115.87 in order to assess and improve the effectiveness of its sexual abuse prevention, detection, and response policies, practices, and training, including by: (1) Identifying problem areas; (2) Taking corrective action on an ongoing basis; and (3) Preparing an annual report of its findings and corrective actions for each facility, as well as the agency as a whole.
(b) Such report shall include a comparison of the current year’s data and corrective actions with those from prior years and shall provide an assessment of the agency’s progress in addressing sexual abuse.
(c) The agency’s report shall be approved by the agency head and made readily available to the public through its website or, if it does not have one, through other means.
(d) The agency may redact specific material from the reports when publication would present a clear and specific threat to the safety and security of a facility, but must indicate the nature of the material redacted.
<i>Data Collection and Review</i> <i>§ 115.89 Data storage, publication, and destruction.</i>
(a) The agency shall ensure that data collected pursuant to § 115.87 are securely retained.
(b) The agency shall make all aggregated sexual abuse data, from facilities under its direct control and private facilities with which it contracts, readily available to the public at least annually through its website or, if it does not have one, through other means.
(c) Before making aggregated sexual abuse data publicly available, the agency shall remove all personal identifiers.
(d) The agency shall maintain sexual abuse data collected pursuant to § 115.87 for at least 10 years after the date of the initial collection unless Federal, State, or local law requires otherwise.
<i>Audits</i> <i>§ 115.93 Audits of standards.</i>
The agency shall conduct audits pursuant to §§ 115.401–.405.
<i>Auditing and Corrective Action</i> <i>§ 115.401 Frequency and scope of audits.</i>
(a) During the three-year period starting on [INSERT DATE ONE YEAR PLUS 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], and during each three-year period thereafter, the agency shall ensure that each facility operated by the agency, or by a private organization on behalf of the agency, is audited at least once.
(b) During each one-year period starting on [INSERT DATE ONE YEAR PLUS 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], the agency shall ensure that at least one-third of each facility type operated by the agency, or by a private organization on behalf of the agency, is audited.
(c) The Department of Justice may send a recommendation to an agency for an expedited audit if the Department has reason to believe that a particular facility may be experiencing problems relating to sexual abuse. The recommendation may also include referrals to resources that may assist the agency with PREA-related issues.
(d) The Department of Justice shall develop and issue an audit instrument that will provide guidance on the conduct of and contents of the audit.
(e) The agency shall bear the burden of demonstrating compliance with the standards.
(f) The auditor shall review all relevant agency-wide policies, procedures, reports, internal and external audits, and accreditations for each facility type.
(g) The audits shall review, at a minimum, a sampling of relevant documents and other records and information for the most recent one-year period.
(h) The auditor shall have access to, and shall observe, all areas of the audited facilities.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(i) The auditor shall be permitted to request and receive copies of any relevant documents (including electronically stored information).
(j) The auditor shall retain and preserve all documentation (including, e.g., video tapes and interview notes) relied upon in making audit determinations. Such documentation shall be provided to the Department of Justice upon request.
(k) The auditor shall interview a representative sample of inmates, residents, and detainees, and of staff, supervisors, and administrators.
(l) The auditor shall review a sampling of any available videotapes and other electronically available data (e.g., Watchtour) that may be relevant to the provisions being audited.
(m) The auditor shall be permitted to conduct private interviews with inmates, residents, and detainees.
(n) Inmates, residents, and detainees shall be permitted to send confidential information or correspondence to the auditor in the same manner as if they were communicating with legal counsel.
(o) Auditors shall attempt to communicate with community-based or victim advocates who may have insight into relevant conditions in the facility.

PREA STANDARDS – FINAL
Adult Prisons and Jails

<i>Auditing and Corrective Action</i> <i>§ 115.402 Auditor qualifications.</i>
(a) An audit shall be conducted by: (1) A member of a correctional monitoring body that is not part of, or under the authority of, the agency (but may be part of, or authorized by, the relevant State or local government); (2) A member of an auditing entity such as an inspector general’s or ombudsperson’s office that is external to the agency; or (3) Other outside individuals with relevant experience.
(b) All auditors shall be certified by the Department of Justice. The Department of Justice shall develop and issue procedures regarding the certification process, which shall include training requirements.
(c) No audit may be conducted by an auditor who has received financial compensation from the agency being audited (except for compensation received for conducting prior PREA audits) within the three years prior to the agency’s retention of the auditor.
(d) The agency shall not employ, contract with, or otherwise financially compensate the auditor for three years subsequent to the agency’s retention of the auditor, with the exception of contracting for subsequent PREA audits.
<i>Auditing and Corrective Action</i> <i>§ 115.403 Audit contents and findings.</i>
(a) Each audit shall include a certification by the auditor that no conflict of interest exists with respect to his or her ability to conduct an audit of the agency under review.
(b) Audit reports shall state whether agency-wide policies and procedures comply with relevant PREA standards.
(c) For each PREA standard, the auditor shall determine whether the audited facility reaches one of the following findings: Exceeds Standard (substantially exceeds requirement of standard); Meets Standard (substantial compliance; complies in all material ways with the standard for the relevant review period); Does Not Meet Standard (requires corrective action). The audit summary shall indicate, among other things, the number of provisions the facility has achieved at each grade level.
(d) Audit reports shall describe the methodology, sampling sizes, and basis for the auditor’s conclusions with regard to each standard provision for each audited facility, and shall include recommendations for any required corrective action.
(e) Auditors shall redact any personally identifiable inmate or staff information from their reports, but shall provide such information to the agency upon request, and may provide such information to the Department of Justice.
(f) The agency shall ensure that the auditor’s final report is published on the agency’s website if it has one, or is otherwise made readily available to the public.
<i>Auditing and Corrective Action</i> <i>§ 115.404 Audit corrective action plan.</i>
(a) A finding of “Does Not Meet Standard” with one or more standards shall trigger a 180-day corrective action period.
(b) The auditor and the agency shall jointly develop a corrective action plan to achieve compliance.
(c) The auditor shall take necessary and appropriate steps to verify implementation of the corrective action plan, such as reviewing updated policies and procedures or re-inspecting portions of a facility.
(d) After the 180-day corrective action period ends, the auditor shall issue a final determination as to whether the facility has achieved compliance with those standards requiring corrective action.
(e) If the agency does not achieve compliance with each standard, it may (at its discretion and cost) request a subsequent audit once it believes that it has achieved compliance.
<i>Auditing and Corrective Action</i> <i>§ 115.405 Audit appeals.</i>
(a) An agency may lodge an appeal with the Department of Justice regarding any specific audit finding that it believes to be incorrect. Such appeal must be lodged within 90 days of the auditor’s final determination.

PREA STANDARDS – FINAL
Adult Prisons and Jails

(b) If the Department determines that the agency has stated good cause for a re-evaluation, the agency may commission a re-audit by an auditor mutually agreed upon by the Department and the agency. The agency shall bear the costs of this re-audit.
(c) The findings of the re-audit shall be considered final.
<i>State Compliance</i> <i>§ 115.501 State determination and certification of full compliance.</i>
(a) In determining pursuant to 42 U.S.C. 15607(c)(2) whether the State is in full compliance with the PREA standards, the Governor shall consider the results of the most recent agency audits.
(b) The Governor’s certification shall apply to all facilities in the State under the operational control of the State’s executive branch, including facilities operated by private entities on behalf of the State’s executive branch.

SCHEDULE E

MDOC VENDOR HANDBOOK FOR VENDOR EMPLOYEES ENTERING A SECURE FACILITY

(Rev. 9-28-2016)

When a Vendor's employees are working under a Contract (#) between the Vendor and the State of Michigan/Michigan Department of Corrections (MDOC), due to safety and security concerns, the following rules apply to all of the Vendor's employees (Employees) working within a MDOC prison/facility. Any violation of the Vendor Employee Handbook may result in a Stop Order being issued against the Employee, the Employee's removal from his/her assignment under the Contract and may result in additional sanctions from the Vendor and/or law enforcement.

Definitions

Contraband: Any article not specifically authorized for admittance into a correctional facility or on facility grounds, e.g. this list includes but is not limited to weapons, any firearm, alcohol, cell phones, cell/electronic watches, iphones, ipads, computers, laptops, tobacco, cigarettes and e-cigarettes, matches, lighters, Tasers®, mace, pepper spray, Google glasses, recording devices, ammunition, handcuff keys, walkie-talkies, yeast, fireworks, etc. (See **Attachment A** for permissible items allowed into a facility without a gate manifest.)

Cell phones, iphones, ipads, computes, laptops, tobacco and tobacco products may be stored in the employee's secured vehicle only while on facility grounds.

Employee Permitted Items. Employees are permitted to take the following items into the facility on their person: a photo ID, up to and no more than \$25.00 currency. See also **Attachment A**.

Discriminatory Harassment: Unwelcome advances, requests for favors, and other verbal or non-verbal communication or conduct, for example comments, innuendo, threats, jokes, pictures, gestures, etc., based on race, color, national origin, disability, sex, sexual orientation, age, height, weight, marital status, religion, genetic information or partisan considerations.

Employee: A person employed by the Vendor.

Facility: Any property owned, leased, or occupied by the Michigan Department of Corrections that is used to maintain custody over a prisoner or parolee, e.g. prison, reentry center, health care area, etc.

Offender: A prisoner or parolee under the jurisdiction of the MDOC or housed in a MDOC facility.

Overfamiliarity: Overfamiliarity, establishing a friendship, mutual attraction or intimate relationship with an offender, is strictly prohibited. Examples are:

- Conduct which has resulted in or is likely to result in intimacy; a close personal or non-work related association,
- Being at the residence of an offender,

- Being at the residence of an offender's family,
- Giving or receiving non-work related letters, messages, money, personal mementos, pictures, telephone numbers, to or from an offender or a family member of a listed visitor of an offender,
- Exchanging hugs with an offender,
- Dating or having sexual relations with an offender, etc.

Over-the-Counter Medication: Medication which can be purchased without a prescription in the United States.

Prescription Medication: Medication which cannot be purchased without authorization from a properly licensed health care authority.

Sexual Harassment of Offenders: Sexual harassment includes verbal statements or comments of a sexual nature to an offender, demeaning references to gender or derogatory comments about body or clothing, or profane or obscene language or gestures of a sexual nature. Sexual harassment is strictly prohibited.

Sexual Conduct with Offenders: The intentional touching, either directly or through clothing, of a prisoner's genitals, anus, groin, breast, inner thigh, or buttock with the intent to abuse, arouse or gratify the sexual desire of any person. Permitting an offender to touch you either directly or through clothing with the intent to abuse, arouse or gratify the sexual desire of any person. Invasion of privacy for sexual gratification, indecent exposure, or voyeurism. An attempted, threatened, or requested sexual act or helping, advising, or encouraging another person to engage in a sexual act with an offender. Sexual conduct with offenders is strictly prohibited.

General Requirements

Discrimination. Employee shall not discriminate against a person on the basis of race, religion, sex, sexual orientation, race, color, national origin, age, weight, height, disability, marital status, genetic information or partisan considerations.

Political Activities. Employees cannot proselytize for any political group or religion in a facility and on MDOC grounds as this may cause safety and security issues within the facility.

Conflict of Interest. If any Employee has a family member or friend who is incarcerated, he/she must immediately notify their supervisor and the MDOC for proper facility assignment.

Public Information. Employees are not authorized to make public statements on behalf of the MDOC.

Role Model. Employees serve as role models to offenders. Therefore, Employees are to act in a professional manner at all times. Any arrest, citation, issuance of a warrant for a felony or misdemeanor offense or issuance of a personal protection order against the Employee must be immediately reported to his/her supervisor. Any action or inaction by an Employee which jeopardizes the safety or security of the facility, MDOC employees, the public or offenders is prohibited.

Fitness for Duty. Employees are required to be physically and mentally fit to perform their job duties. If you do not believe you are mentally or physically fit, please report this issue to your

immediate supervisor. Employees shall immediately notify their supervisor if they are taking medication which may interfere with their work responsibilities.

Use of Leave/Notice of Absence. Employees are required to obtain preapproval of leave from their immediate supervisor. In the event of an unauthorized Employee absence, the Vendor must provide back-up staff.

Punctuality. Employees are required to be punctual and adhere to the work schedule approved by their supervisor and to be at their assignment at the start of their shift. This means that Employees must plan for proper travel time, inclement weather, and to go through the facility check-in process in order to at their assigned location at the start of their shift.

Jail Time or Other Restricted Supervision. No Employee shall be allowed to work in a facility while under electronic monitoring of any type, house arrest, or sentenced to jail time for any reason, including weekends, even if granted a work release pass.

Specific Vendor Employee Rules

1. **Humane Treatment of Individuals.** Employees are expected to treat all individuals in a humane manner while on duty in a facility. Examples of actions of an Employee in violation of this rule include but are not limited to, displaying a weapon, using speech, an action or gesture or movement that causes physical or mental intimidation or humiliation, failing to secure necessary culinary tools, using abusive or profane language which degrades or belittles another person or group, etc.
2. **Use of Personal Position for Personal Gain.** Employees shall not engage in actions that could constitute the use of their position for personal gain. Example, employees are forbidden from exchanging with, giving to, or accepting gifts or services from an offender or an offender's family.
3. **Discriminatory Harassment.** Employees shall not engage in discriminatory harassment which includes but is not limited to, unwelcomed advances, requests for favors, other verbal or non-verbal communication or conduct based on race color, national origin, disability, sex, sexual orientation, age, height, weight, marital status, religion, genetic information, etc.
4. **Misuse of State or Vendor Property/Equipment.** Employees shall not misuse State or Vendor property. Examples: using property for a personal purpose beyond that of your job duties, removing items from the premises without authorization, etc. This includes but is not limited to sexual images and pornography.
5. **Conduct Unbecoming.** Employees shall not behave in an inappropriate manner or in a manner which may harm or adversely affect the reputation or mission of the MDOC. If an employee is arrested or charged with a criminal offense, this matter shall be reported to the Employee's supervisor. Any conduct by an Employee involving theft is not tolerated.
6. **Physical Contact.** Inappropriate physical contact with offenders and MDOC staff is prohibited. Examples include inappropriately placing of hands on another person, horseplay, etc.

7. **Confidential Records/Information.** Employees shall respect the confidentiality of other employees, MDOC staff and prisoners. Employees shall not share confidential information.
8. **Use of Health Care Services.** Employees shall only use the facility health care services in case of emergency, medical stabilization and for serious on-the-job injuries. When the clinic facilities are used for an emergency or on-the-job injury, the Employee is to be transferred as soon as practicable to a physician or hospital.
9. **Insubordination.** Based on the safety and security of the facility, there may be times where Employees are provided guidance from MDOC staff. Willful acts of Employees contrary to MDOC instructions that compromise the MDOC's ability to carry out its responsibilities, are prohibited.
10. **Reserved.**
11. **Searches.** Employees are subject to search while on facility property and prior to entry into a facility. Employees who refuse to submit to an authorized search will not be permitted into the facility.
12. **Emergency.** Employees must immediately respond during an emergency, e.g. call for assistance, respond to an emergent situation, etc. This may include participating in emergency preparedness drills conducted by the MDOC, e.g. fire drills.
13. **MDOC Rules, Regulations, Policies, Procedures, Post Orders, Work Statements.** Employees must be familiar with and act in accordance with MDOC rules, regulations, policies, etc. Employees are prohibited from interfering with and undermining the MDOC's efforts to enforce rules, regulations, etc.
14. **Maintaining Order.** Any action or inaction that may detract from maintaining order within the facility is prohibited, e.g. antagonizing offenders, inciting to riot, etc.
15. **Chain of Command.** Employees shall follow their chain of command. Complaints and concerns are to be submitted to the immediate supervisor unless the situation is an emergency.
16. **Criminal Acts.** Employees shall not engage in conduct that results in a felony or misdemeanor conviction. Employees must provide a verbal report to their immediate supervisor within 24 hours of a felony or misdemeanor citation or arrest, the issuance of any warrant, any arraignment, pre-trial conference, pleas of any kind, trial, conviction, sentencing, federal, diversion or dismissal.
17. **Contraband and Controlled Substances.** There is a zero tolerance policy regarding any Employee possessing, using or introducing controlled substances into a facility where offenders are housed. The possession and presence of contraband presents a safety and security risk and is prohibited. Possession, introduction, or attempting to introduce any substance including controlled substances or intoxicants into any facility is prohibited. Yeast is also prohibited which can be used to manufacture a prohibited or illegal substance.
18. **Use of Alcohol or Controlled Substance.** Employees are prohibited from consuming alcohol or any controlled substance while on duty or on breaks.

Employees who report for duty with alcohol on his/her breath or when suspected of being under the influence of alcohol or a controlled substance, may be prohibited from entering into the facility or be immediately removed from their assignment.

19. Reserved.

20. Introduction or Possession of Contraband. Employees shall not introduce or possess unauthorized items such as escape paraphernalia, weapons, facsimiles of weapons, ammunition, wireless communication devices, cell phones, tobacco, electronic cigarettes, lighters, matches, firearm, alcohol, cell phones, cell/electronic watches, iphones, ipads, computers, laptops, Tasers®, mace, pepper spray, Google glasses, recording devices, handcuff keys, walkie-talkies, yeast, fireworks, etc. Any prisoner who approaches an Employee and requests that contraband be brought into the facility must immediately report the request through his/her chain of command.

21. Motor Vehicles on the Premises of Prison Grounds. All motor vehicles must be properly locked and secured. It is the employee's responsibility to ensure that unauthorized items or contraband are not in the motor vehicle. Motor vehicles on facility grounds may be searched at any time for any reason. Any prisoner who approaches an Employee and requests that contraband be brought onto facility grounds must immediately report the request through his/her chain of command.

22. Reserved.

23. Possession and/or Use of Medication. Employees shall immediately notify their supervisor if taking prescribed medication which may interfere with the Employee's work responsibilities or the safety and security of the facility. Such medication includes but is not limited to: narcotic pain medication, psychotropic medication, mood altering medication and antihistamines. The Michigan Medical Marihuana Act (the Act), Initiated Law 1 of 2008, MCL 333.26421 – 333.26430, allows for the use of medical marihuana for individuals who have been diagnosed with a "debilitating medical condition." It is the position of the MDOC that Employees may not possess or use medical marihuana as it is both a federal and state offense.

24. Reserved.

25. Reserved.

26. Entry into a Facility/Visiting Offenders. Employees are not permitted in non-public areas of the facility for non-work related purposes, especially where offenders are housed.

Generally, Employees may visit an offender only if that offender is an immediate family member and is housed at another facility other than where the employee works, unless the Warden has granted special approval. Employees, who have family members incarcerated in the MDOC, must let their supervisor know immediately who will subsequently report this information to the MDOC. An employee may visit an offender only if that offender is an immediate family member and is housed at a facility other than where the Employee is assigned to work. Immediate family member is defined as a

parent, grandparent, step-parent, grandchild, sibling, spouse, mother-in-law, father-in-law, child, step-child, stepbrother/sister. Visiting an immediate family member who is an offender housed in a facility requires prior permission of both the Vendor and they MDOC.

27. **Dereliction of Duty.** Employees shall fully perform their job duties. Failure to do so is considered dereliction of duty and will be reported to the Vendor.
28. **Use of Force.** Employees shall use the least amount of force necessary to perform their duties. Excessive use of force will not be tolerated. Employees may act to reasonably defend themselves against violence.
29. **Exchange of Duties.** Employees shall not exchange duties or responsibilities with any MDOC staff.
30. **Duty Relief.** Employees shall not leave an assignment without prior relief or authorization from their immediate supervisor.
31. **Security Precautions.** Any action or inaction by an Employee which jeopardizes the safety or security of the facility, MDOC staff, the public or offenders is prohibited. Examples include but are not limited to, loss of equipment (knives, tools), propping open security doors or doors that should remain locked, allowing an unknown or unidentified individual into a building, unauthorized distribution of MDOC exempt policy directives/operating procedures, etc.
32. **Attention to Duty.** Employees shall remain alert while on duty. Sleeping or failure to properly observe an assigned area or offenders are examples of inattention to duty and are prohibited. Items that detract from the alertness of an Employee are prohibited. These items include but are not limited to computer games, books, reading pamphlets, newspapers, or other reading materials while on duty. (MDOC cookbooks, menus, non-exempt policies and procedures and postings, etc. are not considered prohibited items.)
33. **Reporting Violations.** Employees, who are approached by offenders to introduce contraband or violate the safety and security of the institution, shall concurrently report each time they are approached to the Employee's immediate supervisor and MDOC staff. Employees must report conduct involving drugs, escape, sexual misconduct, sexual harassment, workplace safety or excessive use of force. A complete written report of the approach must be made no later than the end of the Employee's work day.
34. **Reserved.**
35. **Reserved.**
36. **Reserved.**
37. **Reserved.**
38. **Reserved.**
39. **Reserved.**
40. **Reserved.**

41. **Reserved.**
42. **Employee Uniform Requirements.** Employees must wear their required uniforms as approved by the Vendor and the MDOC. Employees will not be permitted to enter the facilities without the proper Vendor approved uniform/work attire.
43. **Reserved.**
44. **Reserved.**
45. **Reserved.**
46. **Reserved.**
47. **Falsifying, Altering, Destroying, Removing Documents or Filing False Report.** Employees shall not falsify, alter, or destroy documents or remove documents from the facility. Fraudulent reporting of an Employee's time is expressly prohibited.
48. **Giving or Receiving Gifts or Services.** Employees are prohibited from exchanging with, giving to, or accepting any gifts or services from offenders or an offender's family. This includes but is not limited to food and beverage items, shoe shines, clothing, paper products, stamps, delivering letters/correspondence, etc.
49. **Reserved.**
50. **Overfamiliarity or Unauthorized Contact.** Employees are prohibited from engaging in overfamiliarity with an offender, or an offender's family member or a listed visitor or friend of an offender. Relationships with an offender, other than an Employee with his or her approved family member, is prohibited regardless of when the relationship began. Any exceptions must have Vendor and MDOC prior approval.
51. **Sexual Conduct.** Employees are prohibited from engaging in sexual conduct with anyone while on duty.
52. **Sexual Harassment.** Employees are prohibited from sexual harassing anyone. Employees are prohibited from assisting, advising or encouraging any person to sexually harass another.
53. **Workplace Safety.** Threats made by Employees such as bomb threats, death threats, threats of assault, threats of violence are prohibited. Employees are prohibited from engaging with prisoners in contests like running or sprint challenges, weight lifting contests, etc. Employees shall not physically fight or assault any person on facility grounds. Employees may act to reasonably defend themselves against violence. If an Employee becomes aware of a threat of violence or an act of violence, the Employee shall immediately report this information to their supervisor/chain of command.

Employees will ensure proper storage and handling of tools, keys, equipment, and other items (e.g. metal cans, metallic items).

ACKNOWLEDGMENT

I acknowledge that I have received a copy of, have read, understand and agree to abide by the above additional conditions, including Attachment A. If I have any questions, I will ask my supervisor/manager.

Print Employee Name

Employee Signature

Date

ATTACHMENT A

ALLOWABLE ITEMS WITHOUT GATE MANIFEST

Employees are allowed to bring the following items into a facility while on duty:

1. Driver license/personal identification.
2. Pens (clear) and pencils (no more than two (2) of each).
3. Small notebook.
4. Eyeglasses and sunglasses.
5. Cash, not to exceed \$25.00.
6. Personal keys.
7. One (1) comb, one (1) brush or one (1) pick; non-metal only.
8. One (1) wallet or one purse/bag; no larger than 6" x 8".
9. Umbrella, no pointed tips, no more than 20 inches total length.
10. Feminine hygiene products; one (1) day's supply.
11. One (1) tube lip balm (e.g., Chapstick), one (1) lipstick.
12. Hand cream/lotion (1.6 oz. or less) tube.
13. Non-alcoholic based anti-bacterial hand cleaning sanitizer (four (4) oz. or less).
14. Sunscreen (four (4) oz. or less).
15. Over-the-counter medication; one (1) day's supply limited to pain medication (e.g. aspirin, Tylenol, Ibuprofen) and antacids (e.g. Tums, Mylanta). Over-the-counter medication containing stimulants/relaxants (e.g., NoDoz, Sneeze, NyQuil, Dexitrim) are prohibited. The medication must be factory sealed when brought in and be identifiable.

Note: An Administrative Manifest from the MDOC is required for prescription medication.
16. One individual box/packet (unopened) paper tissues or one handkerchief.
17. Breath mints (one (1) oz. or less), hard candy/cough drops/throat lozenges (one (1) roll or package (six (6) oz. or less) of no more than ten (10) individually wrapped items); Commit nicotine lozenges (or similar brand) (ten (10) or less lozenges).
18. Coffee/tea/creamer/sugar/hot chocolate/coffee filters, soup/hot cereal/powdered drink mix, as described below:

- Coffee – One (1) factory sealed, unopened non-metallic container containing no more than two (2) pounds to be transferred to clear plastic zip bag in presence of gate officer.
 - Tea/creamer/sugar – Single serving, sealed packets or in original packaging and transferred to clear plastic zip bag in presence of gate officer.
 - Hot Chocolate – Maximum of two (2) sealed packets in original packaging and transferred to clear plastic zip bag in presence of gate officer.
 - Coffee Filters – Maximum of one (1) unopened sealed bag in original packaging.
 - Soup/Hot Cereal/Powdered Drink Mix - Sealed packets or envelopes (no more than two (2)).
19. Pocket calendar (non-electronic).
 20. One (1) clear, sealed, unopened plastic container of water not to exceed one (1) gallon.
 21. Contact lens case; wetting solution and/or eye drops (non-prescription) – not to exceed ½ oz.
 22. Factory sealed energy/protein/granola/candy bars – two (2).
 23. Flashlight (mini) and case.
 24. Street shoes during inclement weather to replace snowshoes/boots – one (1) pair.

Schedule F – EASA Worksheet

Enterprise Architecture Solution Assessment	
Contact Info & Purpose (vendor version)	
<p>The purpose of the EA Solution Assessment is to document architectural details of proposed IT solutions in order to determine compatibility with the overall SOM architecture. MDIT/SOM activities which require an Assessment include: the purchase of new licenses, contracting for software development services, purchase of new software components, installation of new software components, the purchase of new hardware components or the use of MDIT staff resources on any project beyond the design phase. All vendor proposals and new contracts must be accompanied by an Assessment, documenting the architectural details of the proposed solution. Vendor should complete all areas except where indicated.</p>	
<p>The Accenture Transformation GPS (TGPS) asset is being used exclusively by the Accenture team. Should MDOC decide to use TGPS on its own at a later stage, the details are provided below. Note that this is a service to provide access to a limited set of MDOC users to the TGPS reporting platform, so a number of responses related to our development and production environment and ways of working are noted as Not Applicable (N/A) below. We are operating under the assumption that these types of information are only applicable for the installation of software or hardware components within the MDOC IT environment, which is not the case here.</p>	
Vendor Version 2.3	
Solution/Project Name	<i>Accenture Transformation GPS</i>
RFP Name/Number	<SOM complete>
Date Submitted	<SOM complete>
Vendor Name	Accenture
Vendor City and State	<vendor complete>
Vendor Phone No.	<vendor complete>
Vendor eMail	<vendor complete>
A brief description of the proposed solution and business purpose/process. (please keep the description brief)	<p><i>Accenture Transformation GPS (TGPS) is a prescriptive analytic for navigating change programs. It consists of a statistically validated survey deployed to a subset of MDOC employees through a cloud-based and secure platform. Responses are uploaded to the platform and results are reviewed in aggregate by key demographic groups. TGPS provides a transformation map to visualization where stakeholder groups are and the dynamics and issues they are dealing with. Prescriptive analytics are then applied to determine an optimal path to a target state on the map for each group. This will be applied to MDOC's transformation program. A handful of MDOC employees will have access to the reporting platform to view results in aggregate to help manage the transformation program. Surveys will be typically every 6-8 months.</i></p>

<p>Additional description of the solution and business purpose. <i>(please expand the row as much as needed)</i></p>	<p><i>See description above.</i></p>
---	--------------------------------------

Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (vendor version)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
1	Server/Application Hosting	Comments
	Internally Hosted	
✓	Externally Hosted	Hosted on third-party Rackspace servers that meet Accenture's security standards
	Internally & Externally Hosted	
2	User Interface Type	Comments (e.g. version or release)
✓	Browser	
	Citrix	
	Client	
✓	Mobile Browser	
	Mobile Client	
	Terminal	
	Other (explain =>)	
3	Supported Browsers (internet)	Comments
	IE 6.0+ (internet, intranet)	
✓	Firefox 3.0.x (internet)	
✓	Chrome 3.0 (internet)	
	Safari 4.x (internet)	
✓	Other (explain =>)	Internet Explorer 10.0+
4	Data Exchange Interface	Comments (e.g. version or release)
	EDI (industry protocol)	
	Flat File (private protocol)	
	Web Service	
	XML	
All N/A	Other (explain =>)	No data exchanged with other systems
5	System Access	Comments
	Internal (SOM only)	
	External (general public)	
✓	External (authorized)	MDOC and user-specific access rights with multi-factor authentication
	Mixed (internal-external)	
6	User Access	Comments

✓	Internet	
	Intranet	
	Local Government (LGNet)	
	Public facing internet	
	Kiosk terminal	
	Vendor Net	
	VPN	
	Other (explain =>)	
(continued)		

Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
7	Data Classification	Comments
✓	Non-sensitive	Depends on deployment approach – Email address or unique employee ID along with simple demographics like location, function, department, career level are captured, as specified by MDOC. However, MDOC can provide a unique key instead if MDOC does not want Accenture to have email address or unique employee ID
✓	Sensitive w/ personal ID info	
	Sensitive w/ no personal ID info	
	Not classified	
	Other (explain =>)	
8	PCI-DSS Compliance Needed?	Comments
	Yes	
✓	No	
9	Data Audit Trail Implementation	Comments
✓	Application Code	
	Database Audit Files	
	Database Triggers	
	Stored Procedures	
	Other (explain =>)	
10	IT Services (Centers of Excellence)	Comments
	x86 Virtualization	
	Address Verification	
	Business Objects Reporting	
	Digital Electronic Gateway (DEG)	
	Extract Transform Load (ETL)	
All N/A	Citrix Virtualization	
11	Enterprise Data Storage	Comments
N/A	<10GB (small)	<i>No data stored on MDOC servers</i>
	10GB-500GB (medium)	
	500GB - 4TB (large)	

	>4TB (x-large)	
12	Database (RDBMS)	Comments
	MS SQL Server 2008	
	MySQL 5.1	
	Oracle 11g	
	TeraData TD 13.0	
✓	Other (explain =>)	PostgreSQL 10.6
(continued)		

Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
13	Database Modeling Tools	Comments
	Erwin 7.x, 8x	
	MSSQL Server Mgmt Studio (match db)	
	MySQL Workbench (match db)	
	Oracle Designer (match db)	
	TeraData Utilities (match db)	
All N/A	Other (explain =>)	
14	Development Framework	Comments
	.NET Framework 3.5, 4.0	
	Java J2EE 5.x, 6x	
All N/A	Other (explain =>)	
15	Development Platform	Comments
	Eclipse 3.x, 4.x	
	Hibernate 3.x	
	IBM Websphere Integration Dev 6.x, 7.x	
	Microsoft SilverLight Expression (match VS)	
	Microsoft Team Foundation System 2010	
	Microsoft Visual Studio 2008, 2010	
	Oracle JDeveloper 11g	
	Spring 2.5	
	Struts 2.x	
	XML Spy 2010	
✓	Other (explain =>)	Ruby on Rails 4.2
16	Development Language	Comments
	ASP .NET 2008, 2010	
	CSS Level 3	
	Microsoft C#	
	Microsoft VB.Net	
	Java	
	JavaScript	

	JDK 6.x, 7x	
	PHP 5.3.x	
✓	Other (explain =>)	Ruby 2.5.1; TypeScript
(continued)		

Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
17	Markup languages	Comments
✓	HTML 4 & 5	
	XML Schema 1.1	
	XSLT 2.0	
	XHTML 2.0	
18	Presentation (Web) Server	Comments
✓	Apache HTTPD 2.x	
	IBM Websphere IHS (match app svr)	
	Microsoft IIS 7.0	
	Other (explain =>)	
19	Application Server	Comments
	.NET Framework 3.5, 4.0	
	Apache Tomcat 7.x	
	IBM WebSphere 7.0, 8.0	
	JBoss 5.x, 6	
✓	Other (Explain)	Phusion Passenger
20	HW Platform	Comments
	Dell	
	HP	
	Sun	
	Unisys Mainframe	
✓	x86 Virtualization	
	Other (explain =>)	
21	Server OS	Comments
✓	Linux Redhat Enterprise Server 5.x, 6.x	

	Linux SUSE Enterprise 11.x	
	Microsoft Windows 2008	
	Unix HP/UX 11i v3	
	Unix Sun Solaris 10.x, 11.x	
	VMWare vSphere 4, 5, VCD	
	Other (explain =>)	
(continued)		
Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
22	Document Management	Comments
	Captaris Alchemy 8.3	
	FileNet Content Services 5.4	
	FileNet Document Mgmt P8	
	HP Trim	
	MS SharePoint Server 2007 EE	
All N/A	Other (explain =>)	
23	Centralized Printing	Comments
	DMB consolidated print center	
All N/A	Other (explain =>)	
24	Testing Tools	Comments
	Junit 4.x	
	LoadRunner 11.x	
	Microsoft Team Foundation System	
	Quick Test Pro 11.x	
	Selenium 1.x, 2.x	
All N/A	Other (explain =>)	
25	Identity Management (network)	Comments
	Active Directory 2008	
All N/A	Other (explain =>)	
26	Identity Management (application)	Comments
	IBM Tivoli SSO (TIM-TAM)	
	Microsoft Active Directory 2008	

All N/A	Other (explain =>)	
27	Project Management	Comments
	Clarity 12.x	
	MS Project 2007, 2010	
	Rational	
All N/A	Other (explain =>)	
(continued)		
Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
	28	Requirements Gathering
	Compuware Optimal Trace 5.x	
	Microsoft Office	
	Microsoft Visio	
	SUITE/SEM templates	
	Rational Requisite	
	Serena Dimensions 2009 R1.x, 11.2	
All N/A	Other (explain =>)	
29	Design Tools	Comments
	Microsoft Visio	
	MSSQL Server Mgmt Studio (match db)	
	Rational Rose	
	Serena Prototype Composer 2009, 2010	
All N/A	Other (explain =>)	
30	Version Control	Comments
	Microsoft Team Foundation System	
	Serena Dimensions (PVCS Mgr) 2009, 12.1	
	Subversion 1.6	
All N/A	Other (explain =>)	
31	Message Queuing	Comments
	Apache Active MQ 5.3	
	IBM Websphere MQ 6.x, 7.x	
All N/A	Other (explain =>)	

32	Business Integration	Comments
	JBoss SOA	
	Websphere Message Broker 6.x, 7.x	
All N/A	Other (explain =>)	
(continued)		
Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
33	Database Tools	Comments
	DBArtisan 8.6, 8.7	
	Infosphere Information Svr v8.1.x	
	MSSQL Server Mgmt Studio (match db)	
	MySQL Workbench (match db)	
	Oracle Developer Suite (match db)	
	Oracle Enterprise Manager (match db)	
	Oracle SQL Developer (match db)	
	Rapid SQL 7.6 & 7.7	
	TeraData Utilities (match db)	
	Toad 9.x & 10.x	
All N/A	Other (explain =>)	
34	Reporting Tools	Comments
	ActivePDF 2009	
	ActiveReports 4.0	
	Birt 3.7	
	Crystal Reports 2008	
	Crystal Xcelsius 2008	
	Crystal Reports for Eclipse	
	MSSQL Reporting Services (match db)	
	Oracle Reports (match db)	
All N/A	Other (explain =>)	
35	End-User Tools	Comments
	Business Objects (BO) XI R2, 3.x, 4.x	
	Oracle Discoverer (match db)	

All N/A	Other (explain =>)	
36	Deployment Tools	Comments
	Microsoft Team Foundation System 2008	
	Serena Dimen.CM Mover 2009, 2.3, 12.1	
All N/A	Other (explain =>)	
(continued)		
Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
37	Build Tools	Comments
	Apache Ant 1.7.x, 1.8.x	
	Apache Maven 2.2, 3.0	
	Microsoft Team Foundation System	
	Serena Dimensions CM Builder 2009 R1.x	
All N/A	Other (explain =>)	
38	Job Schedulers	Comments
	BL/Sched 5.0, 5.2	
	OpCon XPS 4.x, 5.x	
	Tidal Enterprise Scheduler 5.3.1 & 6.x	
	UC4 App Mgr 8.0	
	UC4 Op Mgr 6.0 & 8.0	
All N/A	Other (explain =>)	
39	GIS Technologies	Comments
	ArcIMS 9.3	
	ArcGIS Server 9.3	
	ArcSDE 9.3	
	Erdas ADE Rel. 2	
	ER Mapper Image Server 7.2	
	Oracle Spatial (match db)	
	Oracle MapView (match db)	
All N/A	Other (explain =>)	
40	Issue & Defect Tracking	Comments
	Bugzilla 3.2.5 & 3.4.2	

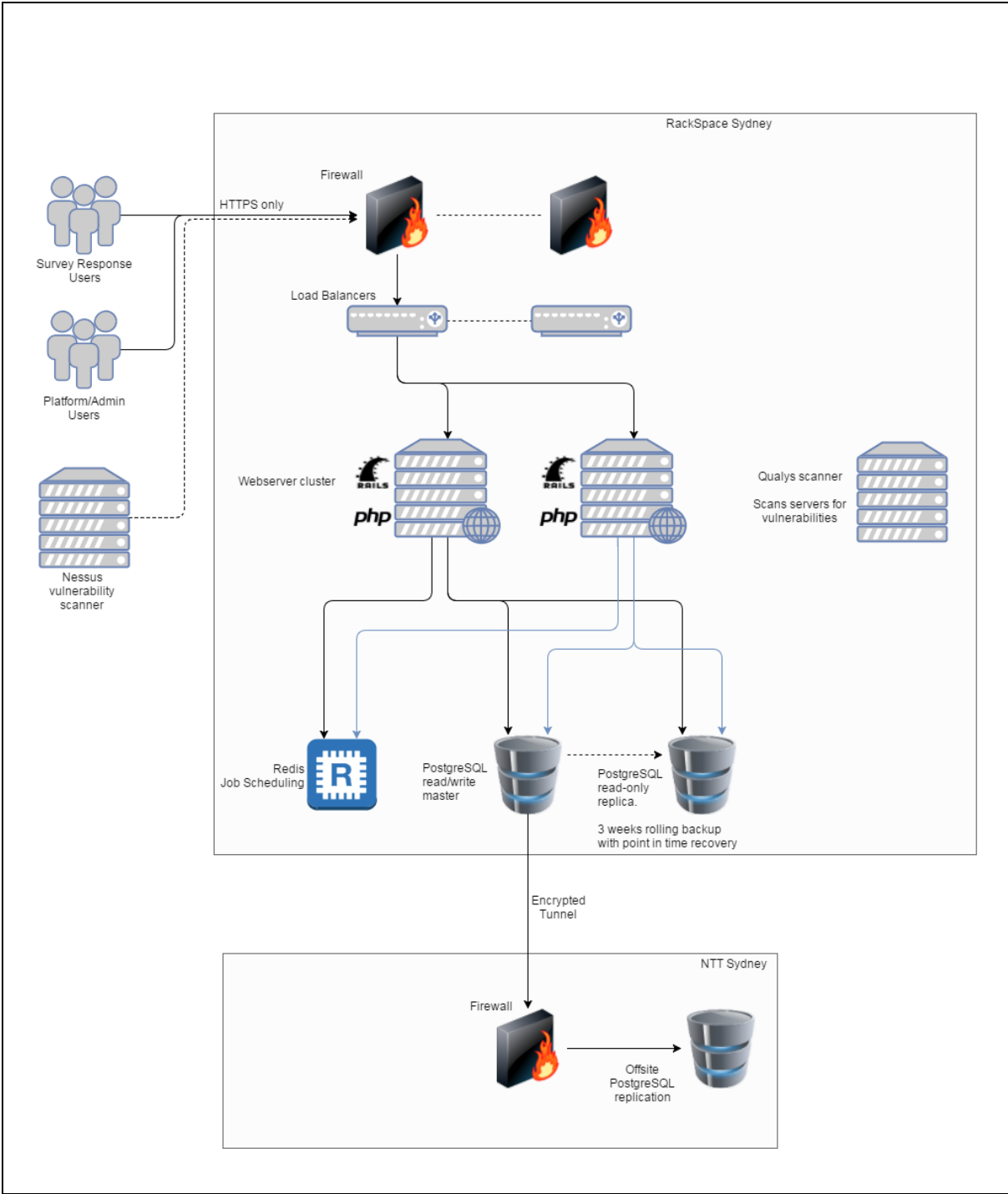
	BugTracker .Net 3.5	
	Clear Quest Chg Mgmt Suite 7.5	
	Microsoft Team Foundation System	
	Serena Mashup Composer 2009 R1.x	
All N/A	Other (describe =>)	
Enterprise Architecture Solution Assessment		
Disaster Planning (Section to be completed by SOM)		
Business continuity requirements.		Describe below
The business requirement(s) that determine the amount of time and the operational availability of the application to the end-user.		Only a handful of MDOC users will have access to the TGPS reporting platform to review results in aggregate, and the access is intermittent, only during 4-6 week stretches following the deployment and closing of the collection window of each TGPS survey. No personal data is provided on the platform is set up for use on a 24x7 basis, but support is only available from the hours listed below as this system does not require such high uptimes.
Select Only One (1)	Availability Requirement Category – Availability Requirement is divided into three different levels. These levels define the continuous service availability requirements of the application. Based on the following definitions, please indicate the level of availability required for this Business Function / Application.	
<SOM>	Urgent - Business Function / Application outage has potential to cause loss of life or risk of injury to a citizen. 99.99% availability (<45 minutes of downtime / month). If an Urgent priority application is not available, DIT will work to resolve the incident 7 x 24 x 365. If the incident occurs after normal business hours, on-call staff (where available) will be called in to resolve the incident. DIT staff will continue to work the issue during and after business hours until the incident is resolved, and the application service restored.	
<SOM>	High – Business Function / Application outage will have a high non-life threatening impact on the public. If this application is not available, there may be an adverse impact on a large number of business clients who use the application. The lack of application availability may also be considered politically sensitive. 99.5% availability (<3.5 hours of downtime / month). DIT will work to resolve the incident 7 x 24 x 365. If the incident occurs after normal business hours, on-call staff (where available) will be called in to resolve the incident. DIT staff will continue to work the issue during and after business hours until the incident is resolved, and the application service restored.	
✓	Medium – Business Function / Application not meeting the Urgent or High criteria will be assigned Medium priority status; this default will be considered the third priority and reflect a situation where there is no risk of personal injury, and the public is not being directly effected. 98% availability (<15 hours of downtime / month). If there is an issue with a medium priority application, work to resolve the incident will be handled during normal DIT Business hours (typically 8:00 am-5:00 pm, Monday-Friday. If the problem is not resolved at the end of the business day, staff will return to work the next business day, and continue the resolution process until the service is restored	
Recovery Point and Time Objectives		

Select Only One (1)	<i>Recovery Point Objective (RPO) is the maximum amount of data loss a business function can sustain during an event.</i>		Select Only One (1)	<i>Recovery Time Objective (RTO) is the maximum amount of time that can elapse until a system / application / function must be returned to service.</i>
	2 hours			2 hours
	4 hours			4 hours
	6 hours			6 hours
	8 hours			8 hours
✓	24 hours			24 hours
	72 hours		✓	72 hours
	Other			Other

Enterprise Architecture Solution Assessment

Server/Network Diagram (vendor version)

Diagrams are useful to illustrate the interaction of technologies. The "Server/Network Diagram" is intended to allow the EA (Enterprise Architecture) Core Team to understand the relationship between the system components. Below is an example illustrating the network components deemed necessary. Vendors may use their own format so long as adequate information is conveyed.



Enterprise Architecture Solution Review
Cost Analysis (vendor version)

Bidder: The intent of the Cost Analysis is to gather an estimate of the long term maintenance and support costs which will be incurred by State of Michigan if the bidders solution is selected. Please complete this section to the best of your ability given the limited information available at this time.

Buyer: If long term cost estimate(s) are requested elsewhere in the RFP please delete this section.

No.	Cost Categories	Cost (\$)	Comments
A.	COTS/Application software update		
	(Includes licensing and updates each year)		
	1. First Year (after one year warranty)		
	2. Second Year		
	3. Third Year		
	4. Fourth Year		
B.	Maintenance and support		
	(includes all programming and DB administration functions for implementing future business requirements)		
	1. First Year		
	2. Second Year		
	3. Third Year		
	4. Fourth Year		
	Total Recurring Cost		

SCHEDULE G - Data Security Requirements

(Contractor's Security Plan is included as an attachment)

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**Contractor Systems**” has the meaning set forth in **Section 5** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

“**FISMA**” means The Federal Information Security Management Act of 2002 (44 U.S.C. ch. 35, subch. III § 3541 et seq.).

“**Hosted Services**” means the hosting, management and operation of the computing hardware, ancillary equipment, Software, firmware, data, other services (including support services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**NIST**” means the National Institute of Standards and Technology.

“**PSP**” means the State's IT Policies, Standards and Procedures located at:

http://michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html

“**PCI**” means the Payment Card Industry.

“**SSAE**” means Statement on Standards for Attestation Engagements.

2. Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Contractor Systems who has sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto (“**Contractor Security Officer**”). The Contractor Security Officer will be considered Key Personnel under the Contract.

3. Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

3.1. the Software must be hosted in a government cloud solution, and Contractor must maintain an annual SSAE 16 SOC 2 Type 2 audit for the Hosted Services throughout the Term maintain FedRAMP certification for the Hosted Services throughout the Term, and in the event the contractor is unable to maintain FedRAMP certification, the State may move the Software to an alternative provider, at contractor's sole cost and expense;

3.2. ensure that the Software is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

3.3. maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in the Contract, and must, at a minimum, remain compliant with FISMA and the NIST Special Publication 800.53 (most recent version) MOD Controls using minimum control values as established in the applicable PSP, and must, at a minimum, remain compliant with FISMA and the NIST Special Publication 800.53 (most recent version) HIGH Controls using minimum control values as established in the applicable PSP;

3.4. provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards;

3.5. take all reasonable measures to:

- (a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein; and
- (b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State's Confidential Information;

3.6. ensure that State Data is encrypted in transit and at rest using AES 256bit or higher encryption;

3.7. ensure that State Data is encrypted in transit and at rest using currently certified encryption modules in accordance with FIPS PUB 140-2 (as amended). *Security Requirements for Cryptographic Modules*;

3.8. ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML) or comparable mechanisms;

3.9. ensure the Hosted Services have multi-factor authentication for privileged/administrative access; and

3.10. assist the State, at no additional cost, with development and completion of a system security plan using the State's automated governance, risk and compliance (GRC) platform.

4. Unauthorized Access. Contractor may not access, and shall not permit any access to, State systems, in whole or in part, whether through Contractor's Systems or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this **Section 4**. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the

Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

5. Contractor Systems. Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor in connection with the Services (“**Contractor Systems**”) and shall prevent unauthorized access to State systems through the Contractor Systems.

6. Security Audits. During the Term, Contractor will:

6.1. maintain complete and accurate records relating to its data protection practices, IT security controls, and the security logs of any of the State’s Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State’s Confidential Information and any other information relevant to its compliance with this Schedule;

6.2. upon the State’s request, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor’s normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State’s option and request, include penetration and security tests, of any and all Contractor Systems and their housing facilities and operating environments; and

6.3. if requested by the State, provide a copy of Contractor’s SSAE 16 SOC 2 Type 2 audit report to the State within thirty (30) days after Contractor’s receipt of such report. Any such audit reports will be recognized as Contractor’s Confidential Information.

6.4. if requested by the State, provide a copy of Contractor’s FedRAMP System Security Plan. The System Security Plan will be recognized as Contractor’s Confidential Information.

7. Nonexclusive Remedy for Security Breach. Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.



Schedule H Correctional Facilities Descriptions

(FY 2019, information is subject to change)

Alger Correctional Facility (LMF), Munising, MI 49862: is a Level II and IV security institution with a total capacity of 896 prisoners, located in Alger County. The prisoner net operating capacity is 888 separated into six housing units. Five are Identical, and the sixth has additional beds. Four housing units are general population and two are used for segregation. Other buildings provide food service, education/programming, warehousing, healthcare, maintenance. storage and space for administrative offices. Staffing for the facility is 240.

Baraga Correctional Facility (AMF), Baraga, MI 49908-9204: is a Level I and V security institution with a total capacity of 868 prisoners, located in Baraga County. The prisoner net operating capacity is 854 separated into eight housing units. One is a 280-bed unit for Level I prisoners. The seven other housing units (four for general population and three for segregation) are inside the secure perimeter and house Level V prisoners. Other buildings house food service, healthcare, prisoner services, maintenance, warehouse, and administration. Staffing for the facility is 357.

Bellamy Creek Correctional Facility (IBC), Ionia, MI 48846: is a Level I, II and IV, Protective and Administrative Segregations security institution with a total capacity of 1,888 prisoners, located in Ionia County. The prisoner net operating capacity is 1,857, which is located within two separate locations. The facility is multi-level housing minimum, medium, close, and general population prisoners. It also houses protective, administrative segregation and temporary segregation prisoners. Prisoners serve Institutional needs in areas such as foodservice, the library, recreational aides, and maintenance workers. Staffing for the facility is 392.

Carson City Correctional Facility (ORF), Carson City, MI 48811: is a Level I, II and IV security institution with a total capacity of 2,248 prisoners, located in Montcalm County. The prisoner net operating capacity is 2,235. The facility consists of seven Secure Level I units with 1,120 beds, three Level II units with 720 beds; two Level IV units with 384 beds, and a 24-bed temporary segregation unit. All units, except temporary segregation, are double bunked. Staffing for the facility is 427.

Central Michigan Correctional Facility (STF), St. Louis, MI 48880: is a Secure Level I security institution with a total capacity of 2,566 prisoners, located in Gratiot County. The prisoner net operating capacity is 2,560. The facility is comprised of 16 separate housing units contained in eight buildings. There are no Individual cells. Prisoner housing units consist of seven to eight bed open bays, 160 prisoners in each of the 16 units. There are separate buildings for administration, food service, school, maintenance / warehouse, and prisoner services. Staffing for the facility is 425.

Charles Egeler Reception and Guidance Center (RGC), Jackson, MI 49201: is a Level I and II reception (Quarantine) security institution with a total capacity of 1,054 prisoners, located in Jackson County. The prisoner net operating capacity is 1,040. This facility sits on 53 acres and houses a separate 119--bed C-Unit for chronic care prisoners as well as the 122-bed Duane L. Waters Healthcare Center. The security healthcare center within the facility provides medical services and food service to both male and female prisoners from many of the state's prisons and camps. Staffing for the facility is 581.

Chippewa Correctional Facility (URF), Kincheloe, MI 49784: is a Level I, II and IV security institution with a total capacity of 2,366 prisoners, located in Chippewa County. The prisoner net operating capacity is 2,340 separated into an East and West side. The East side consists of three Level II housing



units with 240 beds each; one Level IV housing unit with 192 beds; a Level I unit with 144 beds; a 96-bed administrative segregation unit and a 22-bed detention unit. The West side of the facility has dormitory style Level II Housing. There are eight Level II Housing Units which have 140 beds each. The facility includes an administration building, maintenance, power plant and warehouse. There are health care units, food service units and programs/school buildings located on both the East and West sides of the facility. Staffing for the facility is 485.

Cooper Street Correctional Facility (JCS), Jackson, MI 49201: is a Secure Level I security institution with a total capacity of 1,754 prisoners, located in Jackson County. The prisoner net operating capacity is 1,752. This facility serves as a centralized staging point for prisoners transferring to the Camp Program and as a release facility for prisoners who are about to parole, discharge, or transfer to community center placement. The facility is an active member of the MOOC's Community Liaison Committee in the Jackson County area and maintains open lines of communication between the community and prison administration. Staffing for the facility is 282.

Earnest C. Brooks Correctional Facility (LRF), Muskegon Heights, MI 49444: is a Level I, II and IV security institution with a total capacity of 1,246 prisoners, located in Muskegon County. The prisoner net operating capacity is 1,235. The facility sits on 76 acres. Brooks is comprised of six housing units. Three are Level II and house up to 240 prisoners each. Two are Level IV and house up to 192 each. The sixth is Level I and houses up to 120 prisoners. Housing units are separated by additional internal fencing to prohibit prisoners of different security levels from mixing. Other buildings on site include education/programming, food services, health care, administration, maintenance, and warehousing. The facility also has a 22-bed segregation unit. Staffing for the facility is 314.

G Robert Colton Correctional Facility (JCF), Jackson, MI 49201: Is a Level I, Secure Level I, II and IV security institution with a total capacity of 1,842 prisoners, located in Jackson County. The prisoner net operating capacity is 1,812. This facility sits on 114 acres and is a combination of pole barns, which have weatherized buildings, sealed concrete flooring and plaster-board walls, and other buildings that are brick, mortar, steel, and glass. Staffing for the facility is 416.

Gus Harrison Correctional Facility (ARF), Adrian, MI 49221: is a Level I, Secure Level and II security institution with a total capacity of 2,220 prisoners, located in Lenawee County. The prisoner net operating capacity is 2,200. The facility houses prisoners classified to Level I (1,280 beds), Level II (720 beds), and RTP (220 Beds). Staffing for the facility is 463.

Huron Valley Correctional Women's (WHV), Ypsilanti, MI 48197: is a Level I, II and IV security institution with a total capacity of 2,413 female prisoners, located in Washtenaw County. The prisoner net operating capacity is 2,356. The facility serves as the only prison in Michigan which houses females. The facility provides all reception center processing which includes 13 housing units for general population prisoners in level I, II, and IV, Residential Substance Abuse Treatment (RSAT), Residential Treatment Program (RTP), Acute Care, Infirmary, and Detention. Women's Huron Valley services include personnel, prisoner records, business office, maintenance operations, warehouse operations and houses Correctional Mental Health Programs Administration. Staffing for the facility is 644.



Ionia Correctional Facility (ICF), Ionia, MI 49221: is a Level II and V security institution with a total capacity of 706 prisoners, located in Ionia County. The prisoner net operating capacity is 638. The facility is comprised of five Level V housing units and two Level II housing units. Two of the Level V housing units are designated Administrative Segregation, which includes Detention and Temporary Segregation; the remaining three are general population units which include Secure Status Out-Patient Treatment cells. The Level V housing consist of five bi-level, double winged single cell units, consisting of day room area, showers, laundry room, staff offices, barbering services and a fenced-in activity and recreational yard for the security Level V prisoners. The Units designated Administrative Segregation affords prisoner outdoor recreation in single occupancy security exercise modules. The Level II housing consists of a large pole- barn construction divided into two units with 140 beds in each unit. The units have shower, laundry, and recreation areas. The Level II prisoners have separate yard areas, with access to a weight pit, basketball courts, volleyball, baseball, horseshoes, and a running track. Jobs are available for all Level II prisoners. The Prisoner Services building contains classrooms, an auditorium, a gymnasium, a weight room, quartermaster area, barbershop and the general and law libraries. A separate building contains food service, prisoner and staff dining, health care, prisoner property, and maintenance. The administrative building contains the institutions Control Center, Record Office, Business Office, visiting areas, staff training, and a disciplinary and parole board hearing room. Staffing for the facility is 286.

Kinross Correctional Facility (KCF), Kincheloe, MI 49788: is a Level I and II security institution with a total capacity of 1,602 prisoners, located in Chippewa County. The prisoner net operating capacity is 1,593. This facility has the largest fenced area (113 acres currently enclosed) of any state prison in Michigan. The facility includes buildings for administration, two food service operations, education/programming, and maintenance with a power plant. This facility is a regional transportation hub and regional prisoner store hub. Staffing for the facility is 291.

Lakeland Correctional Facility (LCF), Coldwater, MI 49036: is a Level II security institution with a total capacity of 1,466 prisoners, located in Branch County. The prisoner net operating capacity is 1,455. The facility provides mainly dormitory-style housing, each with 16 units including some smaller rooms shared by prisoners who have displayed good behavior while incarcerated. The facility has a separate Foodservice Building, two schools and indoor activity areas. Staffing for the facility is 280.

Macomb Correctional Facility (MRF), New Haven, MI 48048: is a Level I, Secure Level I, II and IV security Institution with a total capacity of 1,422 prisoners, located in Macomb County. The prisoner net operating capacity is 1,400. This facility is comprised of 11 major buildings and two minor buildings, totaling about 300,000 square feet. The prison contains four Level II housing units, one Level IV units and one Level I building outside the security perimeter and one RPT Mental Health Unit. Four other buildings house a school, the administration offices, support services and storage. Staffing for the facility is 337.

Marquette Branch Prison (MBP), Marquette, MI 49855: is a Level I and V security institution with a total capacity of 1,172 prisoners, located in Marquette County. The prisoner net operating capacity is 1,056. The Level V portion of the prison has four General Population housing units and two Administrative Segregation housing units. There are four Level I housing units which are located Just outside the Level V portion of the facility. Buildings include two production kitchens, two chapels, warehousing, education/programming, and maintenance to include a power plant. Staffing for the facility is 382.



Maxey/Woodland Correctional Facility (WCC), Whitmore Lake, MI 48189: is a Level 1 & IV security institution with a total capacity of 377 prisoners, located in Livingston County. The prisoner net operating capacity is 342. The facility has 10 housing pods currently used for MDOC prisoners and a separate unsecure level I unit that houses prisoners that are employed at the facility. An infirmary provides medical services for all prisoners being housed. A food serving area is located within the housing complex and the kitchen is located outside the secure perimeter. Most prisoners have serious mental illness and cannot function adequately in a general prison population. They receive evaluations and treatment services from the Corrections Mental Health Program (CMHP) and are classified into acute care, rehabilitation treatment services, or crisis stabilization services. Staffing for the facility is 338.

Michigan Reformatory (RMI) Reformatory Ionia, MI 48846: is a Level II and IV security institution with a total capacity of 1,237 prisoners, located in Ionia County. The prisoner net operating capacity is 1,215. The facility houses prisoners classified to Level II (472 beds) and Level IV (669 beds) including over 337 outpatient mental health prisoners. The prison is on 40 acres of land 15.6 acres inside the walls. Prisoners serve institutional needs in areas such as food service, yard crews, recreation, institutional housekeeping and maintenance workers. Staffing for the facility is 291.

Muskegon Correctional Facility (MCF), Muskegon, MI 49442: is a Level II and IV security institution with a total capacity of 1,321 prisoners, located in Muskegon Heights. The prisoner net operating capacity is 1,294. There are six general population housing units. The facility also contains a food service building. Staffing for the facility is 243.

Newberry Correctional Facility (NCF), Newberry, MI 49868: is a Level I security institution with a total capacity of 1,108 prisoners, located in Luce County. The prisoner net operating capacity is 1,104 separated into seven interconnected 80-bed units, two-bed housing units, one 88-bed unit, 134-bed unit, a 32-bed housing unit and an adjoining educational building. The facility also contains warehousing, food service, maintenance buildings, and an administration building. All housing units are double bunked, except for four cells that are used for temporary holding. Staffing for the facility is 228.

Oaks Correctional Facility (ECF), Manistee, MI 49660-9200: is a Level II and IV security institution with a total capacity of 1,060 prisoners, located in Manistee County. The prisoner net operating capacity is 1,043. This facility has four double-bunked general population housing units, each housing up to 192 prisoners. There are also three administrative segregation units, including detention. Other buildings include food services, healthcare, a program building, maintenance, warehouse storage and space for administrative offices. Staffing for the facility is 300.

Parnall Correctional Facility (SMT), Jackson, MI 49201-6004: is a Level I security institution with a total capacity of 1,695 prisoners, located in Jackson County. The prisoner net operating capacity is 1,681. This facility is a minimum-security prison that maintains 47 buildings, including five housing units setting on 45 acres. Staffing for the facility is 294.

Richard A. Handlon Correctional Facility (MTU), Handlon Ionia, MI 48846: is a Level II (medium) security facility for male offenders 17 years of age or older with a total capacity of 1,297 prisoners, located in Ionia County. The prisoner net operating capacity is 1,271. The facility houses general population prisoners, along with other prisoners who have been placed in Adaptive Skills Residential Program (ASRP) and the Residential Treatment Program (RTP). The facility houses the largest school system in the correctional system. The academic program is framed with the GED continuum. This includes Adult Basic Education consisting of Reading, Math and English to the eighth-grade level and GED preparation from eighth grade through the tenth-grade level. Supplements to the GED continuum



are Job Skills, Health Education, and Independent Living Skills. Vocational courses include Welding, Auto Mechanics, Machine Shop, Building Trades, Horticulture, and Business Technology. Title One and Special Education are supplemental aids in the adult education segment for prisoners found to be eligible. College correspondence courses are available to students who have completed their academic requirements. The RTP is an integral component of the mental health continuum of care, which includes the outpatient mental health teams, crisis stabilization programs, and inpatient hospital units. The ASRP provides specialized programming in a supportive housing environment to prisoners who have significant limitations in adaptive functioning due to a developmental disability or chronic brain disorder. Staffing for the facility is 324.

Detroit Reentry Center-Parole Location (DRC), Detroit, MI 48212: Detroit Reentry Center is a Level II security location with a total capacity of 1,044 located in Wayne County. The net operating capacity is 1,078. There are 85 prisoner beds that house the dialysis prisoners. There are 987 parolees/probationers that have been returned to receive additional programming and are then released back into the community. The maximum length of stay is 180 days. This facility contains buildings for housing, educational and vocational instruction, food services, a health clinic, dialysis unit, administrative offices, warehouse storage and security. Staffing for the location is 245.

Saginaw Correctional Facility (SRF), Freeland, MI 48623: is a Level I, II and IV security institution with a total capacity of 1,488 prisoners, located in Saginaw County. The prisoner net operating capacity is 1,469. The facility is comprised of 11 main buildings, including three Level II buildings, three Level IV buildings, and one Level I building along with buildings for education, programs, administration, food service, healthcare, warehousing, and maintenance. Staffing for the facility is 298.

Special Alternative Incarceration (SAI), Chelsea, MI 48118: is a Level I security location with a total capacity of 374 offenders located in Washtenaw County. The net operating capacity is 374. The Special Alternative Incarceration program (SAI) began in 1988 as an alternative to prison for male probationers convicted of certain crimes and selected by courts. In 1992, the program was expanded to include both male and female prisoners and probationers. State law precludes participation if convicted of several primarily assaultive crimes. Staffing for this location is 114.

St. Louis Correctional Facility (SLF), St. Louis, MI 48880: Is a Level IV security institution with a total capacity of 1,176 prisoners, located in Gratiot County. The prisoner net operating capacity is 1,144. The facility consists of separate buildings for administration, food service, education, maintenance, storage, and prisoner housing. There are six general population housing units, one is an Adaptive Skills Residential program (ASRP) Unit that provides specialized programming in a supportive housing environment for prisoners. There is one Segregation unit that houses up to 96 prisoners. Staffing for this facility is 315.

Thumb Correctional Facility (TCF), Lapeer, MI 48446: is a Level II security institution with a total capacity of 1,216 prisoners, located in Lapeer County. The prisoner net operating capacity is 1,235. This facility has six housing units including day showers, laundry facilities and staff offices. Four housing units are for adult offenders and two housing units are for youthful offenders. The segregation unit is equipped with stainless steel sinks and toilets, and slotted doors for feeding. Other buildings include the prison services building, which have academic and vocational classrooms, libraries, a barber shop, a food service building for prisoner and staff dining, health care area, warehouse, and maintenance areas. There is an administrative building for staff offices, records, visiting, staff training, hearings, and the institution's control center. Michigan State Industries has a building where it provides industrial laundry services for state and other nonprofit agencies. Staffing for this facility is 309.



Regional Prison Administrators Office

Kincheloe, MI 49788

Staffing: 13

Regional Prison Administrators Office

Jackson, MI 49201-7522

Staffing: 15



FOA Field and Administrative Offices

Alcona Parole/Probation Harrisville, MI 48740 Staffing: 1	Alger Parole/Probation Munising, MI 49862 Staffing: 1	Allegan Parole/Probation Allegan, MI 49010 Staffing: 15
Alpena Parole/Probation Alpena, MI 49707 Staffing: 4	Antrim Parole/Probation Bellaire, MI 49615 Staffing: 2	Arenac Parole/Probation Standish, MI 48658 Staffing: 2
Barry Parole/Probation Hastings, MI 49058 Staffing: 9	Bay Parole/Probation Bay City, MI 48708 Staffing: 21	Benzie Parole/Probation Beulah, MI 49617 Staffing: 2
Berrien Parole/Probation Niles, MI 49120 Staffing: 17	Berrien Probation St. Joseph, MI 49085 Staffing: 27	Berrien Parole Benton Harbor, MI 49022 Staffing: 7
Branch Parole/Probation Coldwater, MI 49036 Staffing: 8	Calhoun Probation Battle Creek, MI 49014 Staffing: 17	Calhoun Parole Satellite Office Albion, MI 49224 Staffing: 1
Calhoun Parole Battle Creek, MI 49014 Staffing: 10	Barry, Branch, and Calhoun Offender Reentry Battle Creek, MI 49014 Staffing: 2	Cass Parole/Probation Cassopolis, MI 49031 Staffing: 8
Charlevoix Parole/Probation Charlevoix, MI 49720 Staffing: 2	Cheboygan Parole/Probation Cheboygan, MI 49721 Staffing: 4	Chippewa Parole/Probation Sault Ste. Marie, MI 49783 Staffing: 5
Clare Parole/Probation Harrison, MI 48625 Staffing: 8	Clinton Parole/Probation St. Johns, MI 48879-1571 Staffing: 5	Crawford Parole/Probation Grayling, MI 49738 Staffing: 2
Delta Parole/Probation Escanaba, MI 49829 Staffing: 5	Dickinson Parole/Probation Iron Mountain, MI 49801 Staffing: 3	Eaton Parole/Probation Charlotte, MI 48813 Staffing: 15



Emmet Parole/Probation Petoskey, MI 49770 Staffing: 6	FOA Region 6 Office Flint, MI 48502 Staffing: 2	Genesee Parole Flint, MI 48502 Staffing: 22
Genesee Probation Flint, MI 48502 Staffing: 51	Gladwin Parole/Probation Gladwin, MI 48624 Staffing: 5	Gogebic Parole/Probation Bessemer, MI 49911 Staffing: 2
Grand Traverse Parole/Probation Traverse City, MI 49684 Staffing: 10	Gratiot Parole/Probation Ithaca, MI 48847 Staffing: 5	Hillsdale Parole Hillsdale, MI 49242 Staffing: 6
Houghton/Baraga/Keweenaw Parole/Probation Houghton, MI 49931 Staffing: 3	Huron Parole/Probation Bad Axe, MI 48413 Staffing: 3	Ingham Probation Lansing, MI 489334 Staffing: 27
Electronic Monitoring Unit Lansing, MI 48910 Staffing: 52	Outstate Territory Administration Lansing, MI 48910 Staffing: 7	Ingham Parole Lansing, MI 48913 Staffing: 15
Ionia Parole Ionia, MI 48846 Staffing: 4	Ionia Probation Ionia, MI 48846 Staffing: 6	Iosco Parole/Probation Tawas City, MI 48764 Staffing: 5
Iron Parole/Probation Crystal Falls, MI 49920 Staffing: 2	Isabella Parole/Probation Mt. Pleasant, MI 48858 Staffing: 15	FOA Regions 5 & 7 Office Mt. Pleasant, MI 48858 Staffing: 3
Hillsdale Probation Hillsdale, MI 49242 Staffing: 5	Jackson Parole Jackson, MI 49202 Staffing: 11	FOA Region 9 Office Jackson, MI 49202 Staffing: 7
Jackson Probation Jackson, MI 49201 Staffing: 23	Kalamazoo Parole/Probation Kalamazoo, MI 49048 Staffing: 48	FOA Region 8 Office Kalamazoo, MI 49048 Staffing: 4
Kalkaska Parole/Probation Kalkaska, MI 49646 Staffing: 4	FOA Region 4b Office Grand Rapids, MI 49503 Staffing: 3	Kent Probation Grand Rapids, MI 49503 Staffing: 51



Kent Parole Grand Rapids, MI 49503 Staffing: 38	Lake Parole/Probation Baldwin, MI 49304 Staffing: 2	Lapeer Parole/Probation Lapeer, MI 48446 Staffing: 9
Leelanau Parole/Probation Suttons Bay, MI 49682 Staffing: 1	Lenawee Parole/Probation Adrian, MI 49221 Staffing: 12	Livingston Probation Howell, MI 48843 Staffing: 11
Livingston Parole Howell, MI 48843 Staffing: 10	Luce Parole/Probation Newberry, MI 49868 Staffing: 1	Mackinac Parole/Probation St. Ignace, MI 49781 Staffing: 2
FOA Region 10 Northeast Office Mt. Clemens, MI 48043 Staffing: 9	Macomb Parole Roseville, MI 48066 Staffing: 26	Macomb Probation Mt. Clemens, MI 48043 Staffing: 102
Manistee Parole/Probation Manistee, MI 49660 Staffing: 4	Marquette Parole/Probation Marquette, MI 49855 Staffing: 6	Mason Parole/Probation Ludington, MI 49431 Staffing: 5
Mecosta Parole/Probation Big Rapids, MI 49307-0239 Staffing: 7	Menominee Parole/Probation Menominee, MI 49858 Staffing: 2	Michigan Department of Corrections Central Office - Grandview Plaza Lansing, MI 48933 Staffing: 505
Midland Parole/Probation Midland, MI 48640 Staffing: 12	Missaukee Parole/Probation Lake City, MI 49651 Staffing: 2	Monroe Parole/Probation Monroe, MI 48161 Staffing: 29
Montcalm Parole/Probation Stanton, MI 48888 Staffing: 11	Montmorency Parole/Probation Atlanta, MI 49709 Staffing: 2	Muskegon Probation Muskegon, MI 49442 Staffing: 27
Muskegon Parole Muskegon, MI 49444 Staffing: 18	Newaygo Parole/Probation White Cloud, MI 49349-0707 Staffing: 7	FOA Region 10 Northwest Office Pontiac, MI 48341 Staffing: 2
Oakland Offender Reentry Pontiac, MI 48341 Staffing: 1	Pontiac Probation Pontiac, MI 48341 Staffing: 62	Troy Probation Troy, MI 48084 Staffing: 49



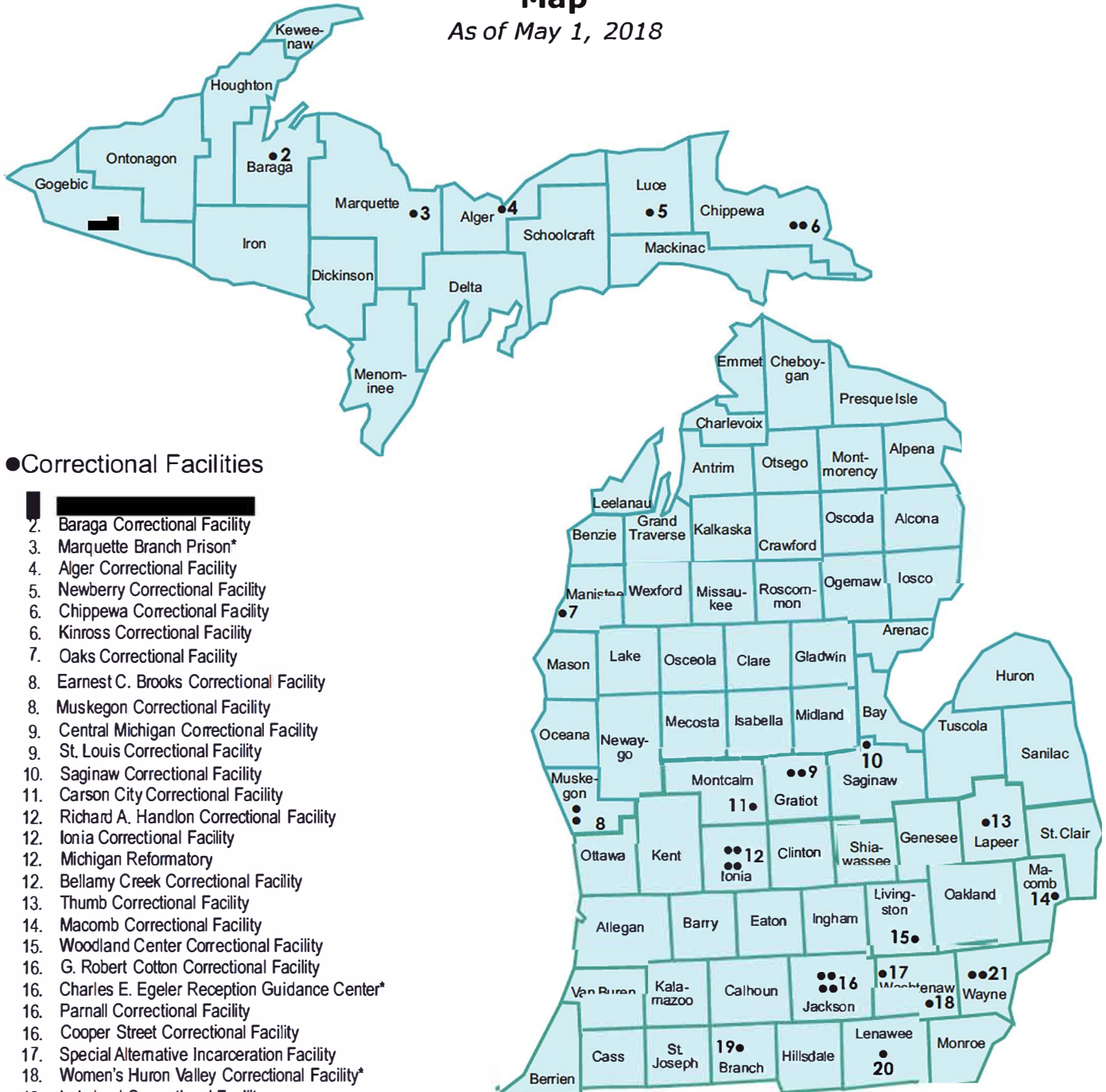
Metropolitan Territory Administration Troy, MI 48084 Staffing: 25	Wayne County Training Troy, MI 4808 Staffing: 1	Pontiac Parole Pontiac, MI 48341 Staffing: 31
Oceana Parole/Probation Hart, MI 49420-1227 Staffing: 4	Ogemaw Parole/Probation West Branch, MI 48661 Staffing: 4	Ontonagon Parole/Probation Ontonagon, MI 49953 Staffing: 1
FOA Regions 1a-4a Office Reed City, MI 49677 Staffing: 6	Osceola Parole/Probation Reed City, MI 49677 Staffing: 4	Oscoda Parole/Probation Mio, MI 48647 Staffing: 3
Otsego Parole/Probation Gaylord, MI 49735 Staffing: 5	Hudsonville Probation Hudsonville, MI 49426 Staffing: 1	Grand Haven Parole/Probation Grand Haven, MI 49417 Staffing: 13
Holland Parole/Probation Holland, MI 49424 Staffing: 12	Presque Isle Parole/Probation Rogers City, MI 49779 Staffing: 2	Roscommon Parole/Probation Roscommon, MI 48653 Staffing: 5
Saginaw Parole Saginaw, MI 48601 Staffing: 14	Saginaw Probation Saginaw, MI 48601 Staffing: 37	Sanilac Parole/Probation Sandusky, MI 48471 Staffing: 4
Schoolcraft Parole/Probation Manistique, MI 49854 Staffing: 2	Shiawassee Parole/Probation Corunna, MI 48817 Staffing: 9	St. Clair Probation Port Huron, MI 48060 Staffing: 15
St. Clair Parole Fort Gratiot, MI 48059 Staffing: 8	St. Joseph Probation Centreville, MI 49032 Staffing: 10	St. Joseph Parole Three Rivers, MI 49093 Staffing: 6
Tuscola Parole/Probation Caro, MI 48723 Staffing: 13	Van Buren Parole/Probation Paw Paw, MI 49079 Staffing: 15	Washtenaw Probation Ann Arbor, MI 48107 Staffing: 26
Washtenaw Parole Ypsilanti, MI 48197 Staffing: 13	FOA Region 10 West Office Lawton Place, 5300 Lawton Staffing: 3	Special Services Unit Detroit, MI 48226 Staffing: 7



Wayne County Parole Detroit, MI 48208 Staffing: 16	Wayne County Parole Electronic Monitoring Detroit, MI 48208 Staffing: 8	Wayne County Parole Specialized Supervision Unit Detroit, MI 48208 Staffing: 10
Wayne County Court Services Unit Detroit, MI 48226 Staffing: 66	FOA Region 10 Central Office Detroit, MI 48226 Staffing: 4	Eastern District Probation Detroit, MI 48215 Staffing: 46
Greenfield District Probation Detroit, MI 48235 Staffing: 46	Lahser District Probation Detroit, MI 48219 Staffing: 47	Chrysler District Probation Detroit, MI 48226 Staffing: 40
Southwest District Probation Lincoln Park, 48146 Staffing: 47	Detroit Detention Center Detroit, MI 48212 Staffing: 66	Detroit Reentry Center Detroit, MI 48212 Staffing: 236
Lincoln Park Parole Lincoln Park, MI 48146 Staffing: 28	Wexford County Parole/Probation Cadillac, MI 49601 Staffing: 7	

Schedule I Michigan Department of Corrections Correctional Facilities Map

As of May 1, 2018




● Correctional Facilities

- 1. [Black Rectangle]
- 2. Baraga Correctional Facility
- 3. Marquette Branch Prison*
- 4. Alger Correctional Facility
- 5. Newberry Correctional Facility
- 6. Chippewa Correctional Facility
- 6. Kinross Correctional Facility
- 7. Oaks Correctional Facility
- 8. Earnest C. Brooks Correctional Facility
- 8. Muskegon Correctional Facility
- 9. Central Michigan Correctional Facility
- 9. St. Louis Correctional Facility
- 10. Saginaw Correctional Facility
- 11. Carson City Correctional Facility
- 12. Richard A. Handlon Correctional Facility
- 12. Ionia Correctional Facility
- 12. Michigan Reformatory
- 12. Bellamy Creek Correctional Facility
- 13. Thumb Correctional Facility
- 14. Macomb Correctional Facility
- 15. Woodland Center Correctional Facility
- 16. G. Robert Cotton Correctional Facility
- 16. Charles E. Egeler Reception Guidance Center*
- 16. Parnall Correctional Facility
- 16. Cooper Street Correctional Facility
- 17. Special Alternative Incarceration Facility
- 18. Women's Huron Valley Correctional Facility*
- 19. Lakeland Correctional Facility
- 20. Gus Harrison Correctional Facility
- 21. Detroit Detention Center
- 21. Detroit Reentry Center

* Includes reception centers

Schedule K – Disaster Recovery Plan

 the #1 managed cloud company	Global Enterprise Security Plan
	Document Name: Business Continuity Plan (BCP) OVERVIEW for Customers
	Document ID: PI-RS-GL-CS-003
APPROVALS	Document Owner: Chuck Rodriguez TRACKING
GES Leadership 23 Apr 2018	This updates Plan dated 28 JUL 2016
MAINTENANCE	
Effective Date:	23 APR 2018
Last Revised Date:	23 APR 2018

1. PURPOSE

This document provides an overview of Rackspace's business continuity plan ("BC Plan") from the customer's perspective. It summarizes routines and precautions undertaken by Rackspace (hereafter referred to as the "Company") to prepare for threats, prevent avoidable damage, and effectively mitigate and recover from significant adverse events that may disrupt or harm key Company processes, systems, operations, and personnel.

Outside the scope of this Business Continuity (BC) Plan Overview for Customers are complete destruction and/or incapacitation of Company-owned facilities and/or network infrastructure. These types of extreme contingencies are addressed through technical risk treatment processes including: wholesale hand-off of data processing and other functions to

To preserve confidentiality and security, this BC Plan Overview for Customers addresses some of the Company's general preparations and response actions. This document provides customers with illustrative information demonstrating strategies and approaches the Company employs to protect and restore critical operations and Company capabilities.

2. COMMITMENT

To assure adequate redundancy, the Company maintains excess capacity across data centers and close partnerships with wholesale data center providers and hardware manufacturers. The Company can quickly secure and employ additional physical operational space, essential equipment, and or qualified talent, to provide Company and customer business continuity and restoration of services to customers. The Company carries excess inventory in its data centers to replace or supplement equipment and is prepared to deploy new IT environments, as needed.

Furthermore, and among its team members and partners, the Company has Design & Build architects and engineers to re-establish and/or restore data center capacity and other services provided to customers.

Customers are responsible for clarifying through their account manager and within their SLA any required BCP customization for their hosted solutions, at additional cost. Disaster Recovery (DR) involves the Company working directly with customers to meet any defined Recovery Time Objectives (RTOs) and/or Recovery Point Objectives (RPOs) that may be agreed to in SLAs. Company Sales Engineers may assist customers define options for customized solutions and services, such as high availability configurations. Otherwise, this BC Plan Overview represents the extent of routine business continuity care provided as a baseline. Business Continuity (BC) at the Company includes preparations to assure the viability and reliability of its internal infrastructure in the face of a major crisis.

3. TESTING

Elements of this BCP are tested in a staggered fashion to minimize any adverse potential impact on customer service delivery. Testing is performed according to a formal schedule.

To preserve confidentiality and assure physical security of facilities and partners, the Company will not share future calendars for or specific results of Data Center (DC) tests. A sample of scenarios tested during the prior year in 2017 is noted below. Each year this document is updated with information from the previous year.

Data Center	Scenario Tested/Experienced in 2017
DFW1	Planned utility service interruption
ORD1	Planned/Unplanned critical internal business systems outage
LON5	Planned utility service interruption
LON3	Building evacuation
IAD3	Planned utility service disruption
SYD2	Building evacuation
DFW2	Planned utility service interruption
HKG1	Severe weather/Natural disaster
IAD2	Planned utility service interruption
ORD1	Building Evacuation
ORD 1	Unplanned utility service interruption
DFW3	Severe weather/Natural disaster
FRA1	Building evacuation
SYD2	Planned utility service interruption
IAD3	Building Evacuation
LON3	Planned utility service interruption
Castle (SAT)	Unplanned utility service interruption
Castle (SAT)	Building evacuation
DFW1	Building Evacuation
ORD1	Unplanned utility service interruption
HKG1	Building evacuation
IAD3	Severe weather/Natural disaster

4. THREAT ANALYSIS

This BC Plan addresses threats identified through a threat analysis process that considers the *likelihood* of incident occurrence and adverse conditions that may produce major impacts. Objectives of the BC Plan are to safeguard the Company’s capacity to protect, respond successfully, and restore through *mitigation* activities key business processes, systems, assets, and/or other essential Company resources required to deliver agreed upon customer services. “Likelihood” does not necessarily suggest that the threat will occur, only that a threat may exist based upon historical evidence and/or industry predictions. “Mitigation” is a risk treatment method – the default represented in this BC Plan Overview.

Threats	Likelihood of Occurrence
Power Utility - Prolonged Outage (DC or a non-DC Company facility)	High
Massive Cyber Attack Unresolved Within RTOs (Network)	High
Effects of Power Utility Outage on Employees (Support Ops)	Moderate
Active Shooter or ‘Lone Wolf’ Attack (Support Ops)	Moderate
Mass Absenteeism Due to Extraordinary Health Impairment Consequent to an Epidemic/Pandemic (Support Ops)	Moderate
Fire Damage to Assets (DC or a non-DC Company facility)	Low
Effects of Fire on Company Personnel (Support Ops)	Low
Severe Weather (DC or a non-DC Company facility)	Low
Effects of Severe Weather that Prevent Employee Assembly or Hampers Their Connectivity (Support Ops)	Low
Destruction of Data Center (Network)	Low
Terrorist Attack by Quasi State or State actors	Low
Localized Electro-Magnetic Pulse (EMP) Caused by solar effects or munitions burst)	Low

5. CRITICAL OPERATIONS

In relative sequence order, the summary of Mission Critical Operations identifies the most significant Company operations for protection, stabilization, response, and recovery to mitigate adverse impacts on customers.

Mission Critical Operations	Locations
Data Center Power and HVAC Operations	TX, VA, IL, London, Sydney, Hong Kong, Frankfurt
All Customer-Facing Communications	All
Major Emergency Support Operations	TX, London
Network Security	All
High-Priority Company Processes, Systems, Assets, and Personnel	All

6. DATA CENTER OPERATIONS

Although the Company's data centers have different configurations to meet customer needs, the statements below apply to all Company essential facilities whether Company run or leased. A focus on key priorities informs Company actions with data centers (DCs) that mitigate disruptions to customer services:

- 6.1 The Company 'commissions' and periodically 'recommissions' all critical systems that impact DC infrastructure performance, including but not limited to: fire suppression, HVAC, electrical, and mechanical systems. On a scheduled basis, all these systems are tested to confirm that they meet both the Company's standards and requirements established by the OEM (Original Equipment Manufacturer).
- 6.2 The Company builds and/or assures redundancy for electrical, mechanical, and safety Systems at each Company owned or leased DC.
- 6.3 The Company conducts regular maintenance according to established schedules that are typically more rigorous than OEM recommendations to assure a sound infrastructure at each DC.
- 6.4 The Company uses a Building Management System to proactively monitor thousands of potential failure points in the infrastructure at DCs. Examples include performance of the cooling systems, electrical breakers, temperatures, and Uninterruptible Power Supply (UPS) batteries. When a capacity or safety threshold is breached, the Company's monitoring systems alert DC personnel in anticipation of actual incidents so that rapid corrective action can be undertaken.
- 6.5 Power — The Company deploys UPS systems in each DC. If commercial utility power fails, the UPS simply accepts the electrical load without disruption. UPS systems only carry load for a defined length of time dependent upon design (i.e., batteries or fly wheel) to support the transfer of load to generators (with at least an N+1 configuration) which are brought online as needed. Some, but not all, DCs have a back-up or parallel utility feed that can be switched on rapidly if the primary commercial utility provider fails or becomes unreliable.
- 6.6. HVAC — Cooling is mission critical in a DC environment. Therefore, large-scale power and capacity-redundant cooling systems are designed to maintain the DC infrastructure as well as each hardware device used by Company customers within acceptable industry-recognized temperature and humidity ranges.
- 6.7 Fire, Flood, Environmental — Each DC complies with local regulatory requirements and building standards for fire, hazardous material and other dangers. The Company tests these systems and monitors sensors regularly, partnering with certified experts so that hardware is maintained up to date and performs at or above required standards. Each DC also uses a raised-floor configuration that mitigates flooding risks.

7. WORLDWIDE CAPACITY

As of January 2018, the Company maintains and contracts with more than a dozen data centers, including new DCs that the Company manages after the acquisition of TriCore and Datapipe. Should a data center be rendered inaccessible to personnel, it can still be

remotely accessed by Company engineering teams. The Company has capacity to rapidly replicate data that was resident at an impacted DC to other data centers within the Company's network and/or contracted centers.

8. NETWORK & SECURITY OPERATIONS

The Company has a large, robust network with full redundancy at Provider/Edge, Core, and distribution layers. If primary hardware on the Company network fails, secondary devices take over automatically. The Company maintains a relationship with multiple Internet Service Providers (ISPs) and can rapidly shift traffic across ISPs should one or more providers experience disruptions and/or performance degradation.

- 8.1 Network Operations Center (NOC) — The Company maintains multiple NOC's and Monitoring tools that proactively scan and manage the health of the Company network. If an intrusion or disruption is detected, monitoring can trigger rapid response that engages NOC and other Company employees to correct issues and lessen the impact on Company infrastructure and its systems. The NOC is staffed 24x7x365 with experienced network engineers and network analysts. Additional qualified Company technical expertise is available on-call to supplement NOC technical responsiveness.
- 8.2 Security — The Company employs logical and physical security protocols to protect its infrastructure and to mitigate denial of service, distributed denial of service, and other attempts to penetrate or disrupt the Company's network infrastructure. Physical security includes biometric scans, surveillance, and restricted access to vulnerable areas. Logical security covers multi-factor authentication, identification access management, and other capabilities (e.g., IPS – intrusion protection systems) accessed by redundant Security Operations Centers – providing 24x7x365 response coverage.

9. MAJOR SUPPORT OPERATIONS

- 9.1 Phone Systems — Each Company support facility is interconnected by Voice over internet Protocol (VoIP) phone switches that route calls automatically if support center operations are temporarily interrupted (e.g., because of personnel evacuation). In the event of an interruption, support technicians at non-impacted locations will automatically receive calls, chats, and customer tickets that would have gone to the interrupted site. The Company has this automated hand-off capability in its San Antonio, Austin and London support operation centers.
- 9.2 Customer Management System (CMS) — The Company's customer management systems are accessible only by authorized Company administrators and engineers at Company locations and via secure virtual private network (VPN) via Internet connection. During an incident, the Company can operate without support technicians needing to be physically present at Company offices. Those customer-facing services can be delivered remotely. This capacity is rehearsed annually as a contingency. CMS and VPN performance are monitored and regularly evaluated. CMS is hosted in one of the Company's DCs and is switchable to backup DC locations in fewer than 30 minutes.
- 9.3 My Rackspace® Portal — The My Rackspace® customer portal is managed only by authorized Company administrators and engineers via secure VPNs. Like the Company's

CMS, the customer portal is hosted at a designated DC and can be switched to its back-up DC location within minutes.

- 9.4 Cloud Control Panel — The Cloud Control Panel is managed only by authorized Company administrators and engineers and can be remotely administered via secure VPN.
- 9.5 Email & Apps Control Panel — The Email & Apps Control Panel is hosted on redundant servers, facilitating scheduled maintenance and avoiding unplanned downtime for customers.
- 9.6 Contingency Capabilities — The Company's support to customers is available 24x7x365. Its support teams are cross trained on systems and back-up solutions. Remote and on-call customer-facing support technicians can assist Company customers, even if those customers' primary support teams are temporarily unavailable.

Company-managed and leased data centers and Company emergency response centers have UPS and generator back up. Additionally, multiple connected Company locations and secure VPN capabilities allow support technicians, operating system (OS) administrators, and account management (AM) teams to work remotely via secured Internet connection to provide customer services, despite facility interruptions.

10. EXPERT & VENDOR PARTNERSHIPS

The Company engages regularly with IT and cybersecurity industry experts for advice and support to respond comprehensively to emergency situations. These best-in-class services providers, threat analysis center counterparts, information technology advisors, and security partners have on-call experts and provide very rapid consultation to help the Company overcome infrastructure impediments.

11. INCIDENT MANAGEMENT OPERATIONS

- 11.1 Incident Management Team (IM Team) — Although the Company has designed its infrastructure to adjust to disruptions of various severity, it works under the assumption that adverse events may occur at any time. The Company maintains a dedicated team of experienced incident management professionals available to respond to any threat to operations. Company employees are trained to alert the IMOC (Incident Management Operations Center) upon discovery of perceived or actual threats launched against Company resources and any other reported damages to the Company. Phishing attacks against Company employees and customers are a type of high-priority threat that is reported routinely to the Incident Management (IM) Team for rapid diagnosis and problem resolution.
- 11.2 Incident Management Process –
 - 11.2.1 Upon receipt of information concerning an elevated threat or an actual incident, the IM Team makes an initial assessment about the severity and impact of the threat/incident. This assessment defines the procedure followed to activate additional preventative steps, mitigate, or recover from the incident. Incidents that impact customers are given the highest priority assessment and may result in an alert (via emails, blog posts, electronic chats, and text messages) to

Company leaders (the "Primary Contacts"). These alerts are also delivered through a reliable and security-vetted third-party vendor not dependent upon the Company's infrastructure.

- 11.2.2 Primary Contacts for the Company are trained specialists, technologists, administrators, engineers, and managers from key functional teams who assemble in person or virtually soon after being alerted. They are charged with mitigating, recovering from, and communicating the impact of an incident.

Primary Contacts include the Event Leader who directs overall mitigation and recovery operations and the Affected Functional Leader(s) who are accountable for mitigation and recovery routines. For example, if a DC lost utility power, the Affected Functional Leader would likely be the head of DC operations or designee. Other Primary Contacts, representing various functions across the Company, are notified according to the type of incident.

Examples of other Functional Contacts include Network Security, Information Technology Operations, Security Support Operations, Product Engineering, Physical Security, and Facilities.

- 11.2.3 IM Training and Drills: Primary Contacts and their respective Backups are trained in crisis management and Company IM procedures. The IM Team conducts scheduled drills to constantly improve response performance.

- 11.2.4 Incident Communications — In the event of an incident, the IM Team typically launches several communication steps:

11.2.4.1 A Primary Contact telephone/video conference bridge is established.

11.2.4.2 An internal blog or secure Chat Room is established for the incident. This coordination channel is made accessible and open to as many who are deemed by the IMOC to be appropriate participants – from support technicians to highly specialized architects and engineers.

11.2.4.3 The Company's internal alert lighting system is changed from Green to Yellow, Red or 'all colors,' depending upon the type and severity of the incident. Company employees are trained about the meaning of the light signals and know to report their availability to support emergency response, as their supervisor may direct – in full coordination with the IMOC.

11.2.4.4 The IM Team, working with the Affected Functional Leader, Support Leaders, the Event Leader and others, determines which customers are or may become impacted by the incident. Once a list of customers at risk is established, communication with them commences. During an incident, this may take several forms including, but not limited to: ticket updates, email messages, customer portal postings, and outbound telephonic advisories from account managers and support technicians.

11.2.4.5 Another channel of communication includes appropriate social networks (e.g., LinkedIn private messaging) for the Company to initially invite Customers Contacts who are not otherwise responding to contact their account team by usual secure methods managed by the Company. Customers are strongly encouraged to rely on secure communication means (e.g., customer portal messaging or via ticket updates) to discuss details about their account status.

11.2.5 Communications Strategy - During an Incident, the IM Team works to update customers whenever new, significant, and relevant information becomes available. In case there is no additional information to share, the IM Team may provide occasional updates to confirm unchanged status continues, or as the situation requires.

The Company's communication approach is designed to be as transparent to customers as possible even though initial information received during an incident can sometimes be ambiguous and incomplete. The Company works to properly balance proactive transparency with measured remediation activities that may, on occasion, result in initial Company communications with some customers that are brief, limited to only verified information.

12. TECHNICAL CHANGE MANAGEMENT

12.1 The Company's technical infrastructure is continuously expanding as Company customer coverage grows. It also evolves in response to issues such as software version upgrades, zero-day patching maintenance, configuration fine-tuning, and other security hardening enhancements. Customers depend upon Company infrastructure reliability to host their most critical applications, data storage, and processing. An inclusive Technical Change Management (TCM) policy and process are in place to protect systems and data from unintended self-imposed disruptions. These TCM precautions greatly reduce the possibility of preventable customer service outages.

12.2 The TCM Program is company-wide and minimizes service downtime by ensuring that requests for changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a structured and consistent manner. All TCM steps are accomplished before any major changes are implemented.

12.3 The TCM Policy applies to all individuals that install, operate, or maintain technical infrastructure. Technical infrastructure includes any shared technology components used in production services.

12.4 The TCM Policy and related processes are administered by the Technical Change Management Team.

12.4.1 Change Advisory Board — Members of the TCM Board are selected for technical expertise they demonstrate, leadership standing within the organization, depth of operational experience, and commitment to the Technical Change Management process. The team meets on a scheduled basis to review requests for proposed significant changes to the Company's infrastructure.

12.4.2 Change Sponsors –The Change Sponsor is accountable to ensure proper technical vetting and functionality. Change Sponsors are responsible for ensuring that the review, preparation, risk assessment, and execution of technical infrastructure changes within their business unit are conducted in a controlled, consistent, and documented manner. Change Sponsors are nominated and selected by the TCM Board.

12.5 Risk Assessment – Changes are assessed using a Risk Priority Number (RPN) Assessment Process that consists of a review of the proposed change across 3 dimensions:

12.5.1 Impact – The potential damage or loss that may be experienced by customers without the change being put into place.

12.5.2 Redundancy – The number of layers of protection in place to insulate customers if change fails.

12.5.3 Likelihood – The probability that something adverse could happen to disrupt the service being changed.

12.6 To conduct an RPN Assessment, an engineer reviews the Impact, Redundancy, and Likelihood of the proposed change. Each statement has an associated Risk Score. The three Risk Scores are multiplied to produce a number between 1 and 1,000. This number is called the RPN Score. The RPN Score determines the level of required approval, the corresponding communication required, and other actions required of the requestor of the technical change.

Nominal changes can be approved by the requesting engineer. Moderate changes require the review and approval of a Change Sponsor. Proposed changes with an RPN Score exceeding a threshold prescribed by the Change Advisory Board must be evaluated by them for approval.

13. EXAMPLES OF THE BC PLAN IN OPERATION

13.1 Severe Weather Event Preventing Company Employees from Reaching a Facility or Data Center

In addition to monitoring the Company's system infrastructure, the IM Team also monitors weather activities at other Company facilities. When a severe weather event is close to or predicted to impact a Company facility within 72 hours, the IM Team will begin providing proactive notification to appropriate Company employees and partners. Various functional teams then initiate their emergency routines. Some of the activities associated with severe weather that may occur include the following:

The IM Team will begin notifying all appropriate Company employees and partners (via bloqs/chat channels, Racker Notification Systems, Conference Bridges, etc.), that a weather event is imminent.

13.1.1 Line managers in all notified sites take a variety of actions including:

- 13.1.1 Notifying unaffected fail-forward sites to adjust schedules to ensure additional resources are available if a possibly impacted site rolls over calls and various work streams for an extended length of time.
 - 13.1.2 Acquiring, refreshing, and/or accessing food/water/emergency supplies for critical staff who are assigned to remain on site during the weather event.
 - 13.1.3 Establishing safety protocols (e.g. identify locations on site to take safe-harbor shelter if required, adjust shift schedules around 'unsafe to travel' timeframes, etc.)
 - 13.1.4 Rescheduling non-essential infrastructure maintenance.
 - 13.1.5 Notifying contingency suppliers/vendors and open communication channels that may be used to activate appropriate 'hip-pocket' 3rd-party service agreements/contracts.
- 13.1.2 DC Operations will make decisions regarding generator fuel supply delivery timing, pre-starting generators in the event of a likely power outage, final verifying that UPS solutions are in place, ready, and checking/activating cellular phone notification rosters to conduct pre-event check-ins for informational accuracy. Cell phones and radios may be used for limited purposes if other routine communication channels are unavailable or become overwhelmed.
- 13.1.3 Because the Company usually does not have a service interruption, it does not provide general notice to all customers. However, a targeted or regional notification may be made if:
- 13.1.3.1 a very strong likelihood exists for an extended or severely damaging weather event,
 - 13.1.3.2 severe damage occurs to Company systems, equipment or personnel that support customers, or
 - 13.1.3.3 inclement weather producing catastrophic effects is predicted or expected to produce collateral conditions that may adversely put customer services at risk.

13.2 Datacenter Utility Power Disruption

On occasion, commercial power supplied to a Company DC may become interrupted. This is a description of what may happen:

When electrical power is completely interrupted, or a low voltage event occurs, the Company's Uninterrupted Power Supply (UPS) is designed to carry the data center's proper electrical load without interruption to customers, while alternative power supplies are brought on line. In DCs where an alternative utility feeder line is available, an automatic transfer switch will assign the electrical load to the alternative utility feed, almost instantly. If the DC is not equipped with a second utility feeder line or the second feed is also interrupted, the DC's generators will be started to provide sufficient power within minutes. The Company's data centers have more than sufficient generator power to operate for an extended length of time; all have backup generator capability. Additionally, Company DCs have fuel supply and standing maintenance contracts that provide for service support to keep generators operational to power the facility.

The Company handles routine power disruption issues seamlessly and routinely without impacting customers. However, if a data center is expected to remain on generator power for a considerable length of time, customers served by the affected DC will be advised and arrangements made to forward-transfer processing loads to excess capacity at one or more other Company data centers.

13.3 Breaker Failure

Large data centers like those managed or contracted by the Company have hundreds of breakers. DC breakers are extremely large and heavy (some weigh over 100 lbs. or 45 kilos) and can carry extremely large voltages. Some of these breakers protect cooling while others protect customer and infrastructure hardware. The purpose of a breaker is to safeguard down-stream infrastructure from damage that might be caused by erratic voltages. When a potentially damaging voltage spike or failure occurs, the breaker 'trips' or opens, shutting off electrical power.

While this is an extremely rare event (usually caused by a mechanical breaker failure rather than an actual incident of erratic voltage), DC monitoring systems alert on-site or on-call engineers who may direct a (a) manual re-route of power, (b) test to close the breaker, thereby re-establishing power, or (c) series of activities to replace the breaker. Then, the DC operations team coordinates immediately with customer support teams who directly update customers. The onsite operations team 're-starts' customer systems that are not already on high-availability configurations.

If an actual disruption to a customer's configuration occurs, the customer is immediately notified by the support team. The support team receives automated monitor alerts and status updates regularly from the IM Team, even as diagnosis and remediation steps proceed. The customer is kept informed in a timely manner.

14. CONCLUSION

While information technology cannot be absolutely guaranteed to escape disruption under extraordinary circumstances, the Company takes extreme care to protect and monitor its processes, systems, assets, facilities, and personnel. Testing and recovery plans and playbooks at the Company's technical and operational business units are developed to ensure on-going readiness and availability of business-critical infrastructure. The Company also engages its key response personnel in scenario-based exercises to address specific most likely threats. When an incident or disruption occurs, the IM Team assumes management lead to speedily diagnose and coordinate resolution of the event and inform customers in a timely manner.

In addition to robust DC facility disaster recovery (DR) plans that are reviewed annually and tested on a rolling quarterly basis, additional emphasis is placed on business continuity and resiliency for processes, people, and technology through Company business unit BC Playbooks for employee training, exercises, and drills. The Company's capacity is in place and evolving for robust incident notification and coordinated immediate action steps via secure channels. The Company's business continuity and resiliency preparations are supported by policy, response team preparation, and the support of the Company's senior leadership. Continuous improvement is integral to Company business continuity and resiliency.

Please contact your Account Team first if you have questions about how this BC Plan Overview applies to your Company account.

15. PLANNED REVIEW / REVISIONS

Item	Description of Planned Revision	Planned Timeframe
01	Annual Document Review	Q1 2019
02	Annual Document Review	Q1 2020

16. REVIEW / REVISION HISTORY

Revision Date	Description	Revised by	Approved By
07/20/2016	Updated / Validated	GDCI/CM/ERM/BCP	CSO
07/24/2017	Updated / Validated	GDCI/CM/ERM/BCP	CSO
04/23/2018	Updated & Reviewed	GDCI/PS/IMOC/BC&R	CSO

Schedule M – Software License

The document below is an example of the license and user agreement associated with the utilization of the Transformation GPS OCM package.

DECEMBER 27, 2018

<<Client Name and Address>>

Re: Transformation GPS

Dear <<Client Name>>:

Accenture LLP (“Accenture”) is pleased to provide this Statement of Work (“Statement of Work” or “SOW”) confirming the services to be provided by Accenture to assist <<the Client>> (“Client”) in connection with Client’s change management project (the “**Project**”). This SOW is subject to the MASTER SERVICES AGREEMENT executed by Accenture and Client as of <<date>> (the “Agreement”). In case of a conflict in terms between this Statement of Work and the Agreement, the terms of the SOW shall prevail with respect to the matters addressed herein only. Capitalized terms not defined herein shall have the meaning described to them in the Statement of Work and Agreement.

1. Background

The change tracking survey (“Transformation GPS”) is to gauge the effectiveness of the change interventions and communications and assess how well the integration activities are progressing with regard to the <<Client’s name and project>>. Client is requesting 4 cycles of Transformation GPS to be conducted on or around:

- ___ February 2019_ and July 2019_ and ___;
- ___ February 2020_ and July 2020; and
- ___ February 2021_ and July 2021 _____.

Each cycle of Transformation GPS will be for a maximum of __3,000_ survey recipients and includes a strategic analysis report (executive summary, key insights, transformation strategy and recommended actions), offshore delivery team support (India-based) and a virtual debrief of results to top leadership for each cycle. The survey can also accommodate up to 8 additional questions; results will be presented as non-benchmarked averages in the reports.

2. Project Objectives

Accenture understands that Client’s objective for the Project is to conduct 6 cycles of Transformation GPS for a maximum for __3,000___ staff for each cycle. Within the parameters of the in-scope Services as specified in this SOW, Accenture looks forward to assisting Client with the Project.

3. Scope and Responsibilities

Scope of Services

The scope of Accenture's Services is to conduct 6 cycles of Transformation GPS, to collect responses from stakeholders in Client's organization, to analyze Transformation GPS data and to provide a Transformation GPS strategic analysis report for each cycle. This "strategic analysis report" will consist of: executive summary, key insights, transformation strategy and recommended actions. In addition, Client will have access for 5-10 people to the Transformation GPS online reporting platform, from which they can view results interactively and export single group PowerPoint reports (team level) and multi-group PowerPoint reports (unit level).

The parties will perform the following Phases:

1. Accenture will work with Client in the **Design Phase** to:
 - Customize the Transformation GPS survey, including the addition of up to 8 additional questions; which results will be presented as non-benchmarked averages in the reports
 - Test the web-based questionnaire
 - Provide Client with survey link
2. Client will then carry out **Collection Phase**:
 - Send out communications/invitations to staff to complete the survey using web-based questionnaires
 - Complete any electronic data input into the Transformation GPS format if paper-based surveys are issued
3. In the **Analysis Phase** Accenture will:
 - Generate a strategic analysis report for the overall target audience (where 6 or more responses in the group are received).
 - Provide the Client with access for 5-10 Client individuals to the Transformation GPS online reporting platform to access results and to export additional PowerPoint reports.
 - Include a 1-2-hour virtual briefing of results and feedback to Client top leadership after each cycle.

Responsibilities

In addition to its other obligations under this SOW, Client is responsible for:

- Defining the target group and providing Accenture with email address and other log in and demographic details
- All communications to staff involved in the Transformation GPS survey
- Tracking and monitoring collection rates and responses to the survey
- Completing any electronic data input into the Transformation GPS format if paper-based surveys are issued
- Developing action planning as a result of the Transformation GPS survey
- Distributing reports to staff and following up
- Arranging availability of Client leadership for Transformation GPS virtual debriefs
- Taking responsibility for action plans as a result of the Transformation GPS survey
- Making reasonable accommodations to occasionally provide a verbal or written reference to prospective clients regarding Accenture's Transformation GPS services

4. Deliverables

The following deliverables (“**Deliverables**”) will be produced by Accenture during the term of this SOW:

- Set up the online survey through a secure https hyperlink;
- 1 x Strategic Analysis Report Deliverable (PPT format); and
- Access to the online reporting platform to export single group and multi group reports for each Transformation GPS cycle, in PPT format

Unless otherwise agreed to in writing by the parties, the above describes Accenture’s complete scope of Services.

5. Assumptions

The following is a list of the assumptions (the "**Project Assumptions**") upon which Accenture has relied upon in agreeing to perform the Services described in this SOW, and which define the legal conditions relating to Accenture's performance under this SOW. Any deviation from the Project Assumptions may cause changes to the Project schedule, fees and expenses, Deliverables, level of effort required, or otherwise impact Accenture's performance of the Services described in this SOW and Accenture shall have no liability with respect to its inability to perform the Services resulting therefrom.

- Client will provide the organization’s demographic data – email addresses or unique identifier data (at the Client’s option) and Client specified demographics e.g. function, geography, career level).
- Client will validate the survey questions, confirm the survey introductory text, draft and review all communications, send communications and follow-up emails.
- In our Project fees we have allowed for the setup of Transformation GPS with the Client organization, and Client access to the Transformation GPS reporting platform for them to review results and export single group and multi group PowerPoint reports.
- We have allowed for web-based collection of survey responses (if paper-based surveys are required, Client is responsible for electronic data input into the Transformation GPS format).
- While we do not expect any expenses will be incurred in conducting Transformation GPS, out of pocket expenses, if any, for travel, accommodation, etc will be billed to Client on a pass-through basis.
- Should additional facilitation, consulting or training days be required, this would be contracted based on our standard daily rates of \$3,000 per day plus taxes, as applicable.
- Decisions to be made by Client will be made promptly and communicated through Client's Project Manager without delay.
- Client's Project Manager will have all necessary authority to commit Client with respect to the subject matter of this Project.
- Client will obtain all consents necessary from third parties required for Accenture to perform its obligations under this SOW. Client shall provide Accenture with access to Client's personnel and facilities sufficient for Accenture to fulfill its obligations under this SOW.
- Client will perform its obligations under this SOW in a timely manner.
- Accenture is not providing any legal advice under this Project. Without limiting the foregoing, Accenture is not providing an interpretation of any laws or regulations that may be applicable to Client or that are otherwise related to the Services being provided hereunder. Client acknowledges and agrees that Accenture has not been retained to provide financial or investment advice, or to make any financial or investment recommendations.
- Client shall provide written instructions to Accenture regarding the giving of appropriate privacy notices to its data subjects. It’s Client’s responsibility to provide notice to data subjects of how their data will be collected and used.

- Client acknowledges that the provision of Services includes benchmarking and improving Accenture’s offerings generally and, as a result, Accenture may anonymize, pseudonymize or aggregate Client Personal Data (“De-Identified Data”) and use or disclose De-Identified Data as part of the Services. Accenture will not associate De-Identified Data with Client’s identity or the personal data of Client’s employees or end users. Client represents and warrants that it has the right to provide the Client Personal Data to Accenture for its use pursuant to this Agreement and Client has provided any necessary notices and obtained any necessary consents from individuals and complied with any notices and any authorizations from governmental authorities as required by applicable law.
- Accenture will access and process Client’s Personal Data from its location(s) as specified in Section 6.3 below.

6. Data Use

6.1 Retention of data in the Transformation GPS database

Accenture shall retain answers to survey questions that are collected by Accenture in the course of providing Services (the “*Answers*”), and Accenture may use the Answers solely to assist with provision of Services and Deliverables, as follows: a) to review and record trends including comparison with data from third parties; b) for analysis and inclusion in the Transformation GPS database for its own records; and c) for any other lawful purposes.

Accenture (i) will not disclose any Answers to third parties (which for the avoidance of doubt does not include Accenture affiliates); (ii) will not identify Client by name unless Accenture is first expressly authorized by the Client to do so; and (iii) may disclose to third parties the fact that Client has used Transformation GPS Services.

6.2 Accenture Data Protocols

For purpose of this SOW, Accenture will access to Client Personal Data (as defined in Schedule 1). Therefore, the parties agree to implement the Data Protection Protocols set out in Schedule 1 – Part B of this SOW.

6.3 Processing Details

(a) Processing Instructions. The Agreement and SOW, including this Addendum, are Client’s complete and final instructions to Accenture for the processing of Client Personal Data.

(b) Subject Matter / Nature / Purpose of the Processing. The subject matter of the Processing is limited to the Client Personal Data identified hereunder. The nature and purpose of the Processing shall be to provide the Services as defined.

(c) Types of Personal Data. The types of Client Personal Data to be Processed by Accenture under this SOW concern the following types of data: email addresses or unique employee identifier and Client’s specified demographics. E.g. function, geography, career level.

Special Categories of Personal Data: The Client Personal Data to be Processed under this SOW does not include any special categories of personal data. **Examples:** Information on racial or ethnic origin, Information on religious or philosophical beliefs, Information on trade union membership, Information on health, Biometric data

(d) **Categories of Data Subjects.** The Client Personal Data to be Processed by Accenture under this SOW concern the following categories of Data Subjects: **Examples:** Employees, Suppliers, contractors or vendors.

Duration of the Processing. Except as otherwise expressly agreed herein or as required by law, the Processing activities carried out by Accenture under this SOW shall not extend beyond the Term of this SOW.

7. Project Fees and Expenses

Accenture will perform the Services on a fixed fee basis. Based on the terms set forth in this SOW, Accenture's fees for its Services as defined above will be \$XXX dollars, plus all applicable taxes, and actual out-of-pocket expenses, including travel and accommodation. Accenture will invoice Client in 3 equal increments as follows:

- March 1, 2019 - \$XXX
- March 20, 2020 - \$XXX
- January 9, 2021 - \$XXX

8. Additional Terms

Notwithstanding anything in the contrary set forth in the Agreement, the parties agree that for the purpose of this SOW, the following provisions shall supersede and apply:

a. Data Protection and Personal Data. Accenture has complied and will continue to comply with its obligations as a data processor arising from the Data Protection Laws (as defined in Schedule 2) in force from time to time to the extent that those obligations are relevant to this Agreement. Client will likewise comply with its obligations as a data controller. Further, Accenture and Client have each implemented and shall maintain an information security program including reasonable administrative, technical and physical measures designed to secure and protect the confidentiality, integrity and availability of all Confidential Information while in such party's possession against unauthorized, unlawful or accidental access, disclosure, transfer, destruction, loss or alteration. Accenture will process Client Personal Data in connection with the Services, therefore the parties agree on the general responsibilities (with respect to e.g. nature and purpose of such access, security controls and protocols, international transfer of data) as set out in Schedule 2. Client as the data controller is responsible for determining (i) if Client will be able to comply with applicable data privacy laws in its use of the Services and (ii) whether data privacy laws require that Client's Personal Data originating from a particular country remain inside that particular country ("Localization"). In the event that Client determines that Localization is required to enable Client to comply with applicable Client Laws, Client shall notify Accenture and the parties agree to negotiate in good faith additional costs associated with such Localization. Accenture shall be entitled to rely on Client's Localization determination. If Localization is not technologically feasible, the parties will in good faith discuss workarounds.

b. Warranties: Accenture warrants that its Services will be performed in a good and workmanlike manner, in accordance with the SOW, and that Deliverables will materially comply with their applicable specifications. Accenture will re-perform any work not materially in compliance with this warranty which is brought to its attention within thirty (30) days after that the work has been performed. In addition, each party warrants that upon its execution, this MSA or any SOW will not materially violate any term or condition of any agreement that such party has with any third party and that the officers executing this MSA or a SOW are authorized to bind such party to the terms and conditions hereof. The preceding are the only warranties and over-ride all other warranties, conditions and representations, express or implied, including fitness for purpose, merchantability, non-infringement or otherwise. Client warrants to Accenture that it has all necessary rights to provide the Client Personal Data to Accenture for the processing to be performed in relation to the Services. Client shall be responsible for obtaining all necessary consents, and providing all

necessary notices, as required under the applicable Data Protection Laws (as defined below) in relation to the processing of the Client Personal Data. The Services do not include the provision of third-party products, nor address any legal or regulatory issues concerning the Client's operations or use of the Deliverables. The '*applicable Data Privacy Law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established.

c. Liability. Accenture's sole liability for any claim under or in relation to this Agreement (however arising, including under negligence) shall be the payment of direct damages of the Client and such damages for any such claim shall not exceed an amount equal to the fees received by Accenture with respect to the work that is the subject matter of the claim and, notwithstanding the above, such damages for all claims in any manner related to the Agreement shall not in the aggregate exceed an amount equal to the fees received by Accenture under the Agreement (if the term of the SOW is 24 months or longer, the amount of the aggregate cap shall be limited to the fees received during the 12 month period immediately preceding the event giving rise to the first such claim).). In no event will either party be liable (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any: (i) consequential, indirect, or punitive damages, or (ii) loss of profits, business, opportunity or anticipated savings (whether directly or indirectly arising). Nothing herein excludes or limits either party's liability to the other which cannot lawfully be excluded or limited.

d. Rights in Deliverables: Each party (or its licensors as applicable) shall retain ownership of its intellectual property rights, including without limitation patents, copyright, know-how, trade secrets and other proprietary rights ("IP") which were existing prior to each respective SOW, or IP developed, licensed or acquired by or on behalf of a Party or its licensors independently from the Services or the Deliverables, in each case, including any modifications or derivatives thereof which may be created as part of the Services (collectively "Pre-Existing IP"). Client hereby grants to Accenture (and its subcontractors), during the term of this SOW a non-exclusive, fully paid, worldwide, non-transferable, limited license to use Client's Pre-Existing IP (and shall obtain the same license/consent as required from any third party), solely for the purpose of providing the Services and Deliverables. All IP in the Deliverables remain in and/or are assigned to Accenture. Effective upon final payment (including any license fee specified in the SOW), Accenture hereby grants to Client, subject to any restrictions applicable to any third-party materials embodied in the Deliverables, a perpetual, worldwide, nontransferable, non-exclusive, irrevocable right and license to use, copy, modify and prepare derivative works of the Deliverables for purposes of Client's and its affiliated companies' internal business only. Accenture Pre-Existing IP embedded in Deliverables may not be used separately. Each party is free to use concepts, techniques and know-how retained in the unaided memories of those involved in the performance or receipt of the Services. Accenture is not precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the Deliverables provided and to the extent that they do not contain Client Confidential Information. Client agrees, notwithstanding any provision to the contrary, that Accenture has the right to anonymize and aggregate Client data with other data and leverage anonymous learnings and insights regarding use of Accenture products and/or services (the anonymized data, "Accenture Insights

Data” or “AID”), and that Accenture owns AID and may use AID for any business purpose during and after the term of this Agreement (e.g., to develop, provide, and improve Accenture products and services).

9. Cloud Services

Client acknowledges that certain aspects of the Services are provided by a hosting service provider: Rackspace (the “Cloud Vendor”). This part of services is later referred as “Cloud Services”. Client acknowledges that any changes to the Cloud Services could impact the provision of the Services by Accenture to Client.

10. Project Approach

Work on the Project will be performed virtually for survey design and execution and in the Client offices if possible for the leadership debriefs. The estimated timeframe established for performance of the Services is 6-8 weeks per cycle commencing from <<Date>>_____ (“**Term**”).

Accenture appreciates the opportunity to be of service to Client and looks forward to working with you on this challenging Project. If this SOW is consistent with your understanding and acceptable to Client, please sign where indicated and return a signed copy to the undersigned at your earliest convenience.

Very truly yours,

Accepted and Agreed:

ACCENTURE LLP

Signed: Name and Title (Printed or Typed)
Managing Director

Signed: Name and Title (Printed or Typed)

Address (Printed or Typed)

Address (Printed or Typed)

Date

Date

Schedule 1
Data Protection

Part A – General

1. Definitions: the capitalized terms used in this schedule are defined as follows:

“**Client Personal Data**” means personal information (as defined in the applicable Data Privacy Laws) owned or controlled by the Client, which Accenture has access to or otherwise processes for the purpose and during the provision of the Services.

“**Client Personal Data Protection Protocols**” means the organizational measures to protect Client Personal Data against unauthorized use, destruction or loss, alteration, disclosure or access (which measures will constitute “reasonable steps to protect” as required by the applicable Data Privacy Laws).

“**Data Protection Laws**” means all applicable data protection and privacy laws that apply to the processing of personal data under this Agreement.

“**Process**” means, with respect to Client Personal Data, to access, collect, use, store, manipulate, disclose, transfer, analyze or destroy any such data, or as otherwise defined in the applicable Data Privacy Laws (and “Process” and “Processing” will be construed accordingly).

The parties acknowledge that, with respect to all Client Personal Data Processed by Accenture for the purpose of providing the Services under this Agreement: the Client will determine the scope, purposes, and manner for which such Client Personal Data may be accessed or processed by Accenture, and Accenture will limit its access to or use of Client Personal Data to that which is necessary to provide the Services, comply with applicable laws, or as otherwise directed by the Client (to the extent such directives do not cause Accenture to be in breach of applicable law). Accenture shall be authorized to act and rely on, and shall implement, each Client directive in the performance and delivery of the Services as agreed by the Parties in accordance with the change order procedures. Client shall be responsible for any fines or penalties imposed on Accenture or Client by a governmental authority resulting from Accenture's failure to comply with Compliance Directives to the extent such fines or penalties result from Client's failure to respond, within a reasonable period of time, to a written request by Accenture for interpretation of any Client Law or Compliance Directive; and b) the Client will be responsible for determining and monitoring its compliance with Data Privacy Laws, and Accenture will not be required to monitor or advise the Client regarding Data Privacy Laws. For the avoidance of doubt, Accenture must not take on responsibility to implement, monitor and/or ensure compliance with data privacy laws applicable to Client during the performance of the Services;

2. Accenture will maintain procedures to detect and respond to loss, misuse, or unauthorized acquisition of Client Personal Data while such data is in Accenture's custody or control. Accenture will, where so required by applicable Data Privacy Laws promptly notify the Client of a loss, unauthorized acquisition, or misuse of unencrypted Client Personal Data in Accenture's custody. Accenture will promptly make available to the Client appropriate details of the unauthorized acquisition or misuse and shall use commercially reasonable efforts to investigate and prevent the recurrence of such unauthorized acquisition or misuse of the Client Personal Data. The parties will reasonably cooperate to remediate security incidents and prevent their recurrence. The Client, in its sole discretion, will determine whether and when to notify any individuals or persons (including governmental authorities) regarding any security incident affecting Client Personal Data.

The parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Data under this SOW:

- (a) Accenture will process the Client Personal Data only in accordance with Client's documented processing instructions as set forth in this Agreement. Accenture shall inform Client if, in Accenture's opinion, any Client instruction infringes any applicable Data Protection Law.
- (b) All Accenture personnel, including subcontractors, authorized to process the Client Personal Data shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.
- (c) Each party shall implement appropriate technical and organizational security measures to safeguard Client Personal Data from unauthorized processing or accidental loss or damage, as further described in this Schedule 2 – Part B. Client acknowledges and agrees that, taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Data, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in this Schedule 2 – Part B provide a level of security appropriate to the risk in respect of the processing of the Client Personal Data.
- (d) Client specifically authorizes the engagement of Accenture's affiliates as sub processors and generally authorizes the engagement of other third parties as subprocessors as identified herein. Accenture shall contractually require any such sub processors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder. Accenture shall remain fully liable for the performance of the subprocessor. Accenture shall provide Client with written notice of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the parties shall be resolved via the contract dispute resolution procedure.

- (e) Taking into account the nature of the processing, Accenture shall provide assistance to Client as reasonably requested in responding to requests by data subjects to exercise their rights of access, rectification, erasure, portability, and the right to restrict or object to certain processing. Client shall be responsible for the reasonable costs of such assistance.
- (f) Taking into account the nature of the processing and the information available to Accenture, Accenture shall provide assistance to Client as reasonably requested with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to notify regulators and data subjects of a breach with respect to Client Personal Data as required by law; (iii) Client's obligation to conduct data protection impact assessments with respect to the processing as required by law; and (iv) Client's obligations to consult with regulators as required by law. Client shall be responsible for the reasonable costs of such assistance.
- (g) Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in this Section and submit to audits and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the confidential information of Accenture and its other clients.
- (h) Upon expiration or termination of the Services, Accenture shall return or destroy any Client Personal Data in accordance with the terms and timelines agreed by the parties, unless otherwise required by applicable laws. Unless otherwise agreed, Accenture will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.
- (i)

Part B – Procedures for the Protection of Client Personal Data

These Data Protection Procedures ("Procedures") set forth the security protocols that Client and Accenture will follow with respect to maintaining the security and privacy of Client Personal Data in connection with the applicable services agreement in place between the Parties ("Agreement").

1. General

In the event of a conflict or inconsistency between the terms of the Agreement and the terms of the Procedures, the Procedures shall govern. In the event of a conflict or inconsistency between the terms of these Procedures with the terms of any Attachments, the terms of the Procedures shall govern. Capitalized terms used herein, but not defined shall have the meanings ascribed to them in the Agreement.

2. Security Policy

Accenture will maintain globally applicable policies, standards, and procedures intended to protect Accenture and Client data, which will be provided upon Client's request. Such policies include, but are not limited to:

- a) System Security
- b) Security of Information and Acceptable Use of Systems
- c) Confidentiality
- d) Data Privacy
- e) Data Management

3. Global Access

Accenture may access the Client Personal Data from anywhere within Accenture's Global Delivery Network, unless otherwise mutually agreed by the Parties.

4. Organizing Information Security

4.1 Accountability

The following executives from the Client and Accenture shall be responsible for confirming the implementation of and ongoing compliance with these Procedures. Any notices under these Procedures or the Agreement regarding the Client Personal Data obligations of each party should be as follows: communications regarding the day-to-day obligations should be communicated in writing via e-mail or other written notice to each of the Data Protection Executives and communications regarding any changes to the terms of these Procedures (including any Attachments) or the terms of each Party's Client Personal Data obligations under the Agreement should be directed as required under the notice provisions of the Agreement with copies provided to the Data Protection Executives.

- Client Data Protection Executive: **[INSERT NAME, TITLE AND CONTACT INFORMATION]**
- Accenture Data Protection Executive: **<<Managing Director Name>>, Managing Director**

The Data Protection Executives will jointly review these Procedures at a minimum on an annual basis to identify if any changes are necessary. Client will remain responsible for Client-controlled systems. Each party will be responsible for complying with each Safeguard designated as its responsibility in the below table, as the Safeguard relates to a party's employees, subcontractors, and owned-equipment, in its control and used to perform their respective obligations under each Statement of Work. Each party will promptly notify the other party of any suggested changes to the application of agreed upon Procedures or other general concerns about potential gaps in the information security environment.

Any material changes to these Procedures must go through the change control procedures as set forth in the Agreement.

Control		Responsible Parties	
		Accenture	Client
5.0	Asset Management		
5.1	Acceptable Use of Assets		
5.1.1	Comply with any written Client-provided guidelines for use of Client-provided devices that may be used to access Client Personal Data.	X	
5.2	Information Classification		
5.2.1	For each covered statement of work, the Client shall appropriately inform Accenture of the types of Client Personal Data that Accenture will process. Client will notify Accenture when Client Personal Data is being provided and label it clearly and appropriately.	X	X
6.0	Human Resources Security		
6.1	Training		
6.1.1	Require all Accenture project personnel to complete standard Accenture and any Client provided data protection training.	X	
6.1.2	Require all Client project personnel to complete training on the Procedures herein.		X
7.0	Physical and Environmental Security		
7.1	Physical Security		
7.1.1	Implement physical security controls per location security standard where Client Personal Data is being Processed.	X	X
7.1.2	All personnel shall be registered and required to carry appropriate identification badges.	X	X
8.0	Communications and Operations Management		
8.1	Network Security Management		
8.1.1	Maintain Access Control Lists (ACLs) for network devices.	X	X
8.1.2	Network traffic shall pass through firewalls that are monitored and protected by intrusion detection/prevention systems that allow traffic flowing through the firewalls to be logged.	X	X
8.1.3	Access to network devices for administration shall require a minimum of 128-bit encryption.	X	X
8.1.4	Anti-spoofing filters shall be enabled.	X	X
8.1.5	Network, application, and server authentication passwords will meet each party's complexity guidelines.	X	X
8.1.6	Enable Transport Layer Security (TLS) between the Client and Accenture email domains.	X	X
8.2	Virtual Private Networks ("VPN"). When remote connectivity to the Accenture network is required for		

	Processing of Client Personal Data and site to site VPN has been agreed upon, both parties shall deploy VPN servers with the following or similar capabilities:		
8.2.1	Connections will be encrypted using a minimum of 128-bit encryption.	X	X
8.2.2	Client connections to the Accenture Service Locations will only be established using the Accenture VPN servers.	X	X
8.2.3	Split tunneling shall be disabled.	X	X
8.2.4	Require the use of two-factor authentication.	X	X
8.3	Media Handling		
8.3.1	When transferring Client Personal Data:		
8.3.2	Implement a minimum of 128-bit encryption of data unless restricted by local regulations or agreed to by both Parties.	X	X
8.3.3	Use of portable media to transfer Client Personal Data should be avoided if possible. When necessary, transfers of data on recordable or portable media must be encrypted at all times while in transit, with encryption keys transported or transmitted separately; and all Client Personal Data transmitted between the Parties will be conveyed using a secured and encrypted storage device or file transfer mechanism as agreed by the Data Protection Executives. A minimum of 128-bit encryption is required. Intercompany email should be avoided if at all possible.	X	X
8.3.4	Where commercially practical and as agreed upon by the Data Protection Executives, the Client shall implement means such as masking or de-identification of Client Personal Data prior to providing access to Accenture. The Client must identify instances where unmasked/unscrambled production data is used outside of production environments before providing Accenture access. If production data is used for testing, compensating controls shall be agreed to and employed.		X
8.4	Physical Transport of Data		
8.4.1	Use a professional grade courier with logged chain of custody for any third-party transport of hard copy or mobile media containing Client Personal Data.	X	X
8.5	Data Disposal		
8.5.1	Upon leaving the project, project team members will return or destroy any Client Personal Data that is in his or her possession.	X	
8.5.2	Accenture may retain archival copies of records containing Client Personal Data as reasonably necessary or as part of normal backup processes to verify Accenture's compliance with this Agreement. Accenture will identify such data to Client at the time such archival copies are withheld and shall mask or otherwise redact the Client Personal Data in those records. Accenture shall not be obligated retain archival copies of Client databases, or other compilations or stores of Client Personal Data.	X	

8.5.3	Accenture shall destroy hard copies containing Client Personal Data via shredder or by depositing in a secure destruction bin when no longer required in the performance of the Services.	X	
8.6	Third Party Service Delivery Management		
8.6.1	Execute substantially similar contractual terms relating to privacy and security with subcontractors retained to provide the Services.	X	
8.6.2	Maintain commercially reasonable contractual terms relating to privacy and security with enterprise information technology and communications suppliers who are engaged to provide general services to Accenture and are not engaged specifically to provide the Services (e.g. email and telecommunications providers).	X	
8.7	Back-up		
8.7.1	If Accenture provides hosting services for production databases and offsite tape backups are used, then the backups will be encrypted, at a minimum of 256-bit encryption unless there are contradictory legal requirements, at the Client's expense.	X	X
9	Access Control		
9.1	User Access Management		
9.1.1	The Client shall use reasonable commercial efforts to restrict Accenture's access to only that Client Personal Data required for Accenture to perform its obligations under the Agreement.		X
9.1.2	Implement user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to all client systems, client data and all internal applications used during the course of the project. Designate an appropriate authority (as defined by the engagement) to approve creation of new user ID, or elevated level of access for existing ID.	X	X
9.1.3	Implement an engagement level access control roster capturing the access details for engagement resources, covering type of access, date access granted, and date access revoked for team members.	X	
9.1.4	Review the access control roster at least quarterly, or as otherwise agreed to by the Parties in writing, to confirm that access levels are still appropriate for individual roles and to confirm that access revocations for personnel who departed from the engagement have been processed correctly.	X	
9.1.5	Revoke access for personnel departing the engagement within two business days of departure, or in compliance with contractual obligations, whichever is sooner.	X	X
9.1.6	When applicable, provide access for project personnel and other applicable personnel using the concept of Least Privileged Access, meaning individuals are only granted access to those resources and systems that are required to perform their role.	X	X

9.1.7	When applicable, logically separate access between environments (e.g., development, testing, and production) so that an individual can be granted access to one environment without being able to access others.	X	X
9.1.8	Provide each individual accessing a system or application with a unique user ID and password. Prohibit user IDs and passwords from being shared.	X	X
9.1.9	Provide two-factor authentication to access the Client's internal network environment from non-Client/non-Accenture locations. An internal network environment generally means the network environment that what would be available if an individual is sitting within the Client's offices or data centers.	X	X
9.1.10	To the extent possible, the Client will enable access methods to control offloading, printing, copying, pasting, or other methods of data extraction of Client Personal Data (e.g. Citrix/VDI/application layer firewall).		X
9.2	Password Management		
9.2.1	Electronic communications of passwords must be encrypted using a minimum of 128-bit encryption.	X	X
9.2.2	Require initial user passwords to be changed during the first logon. Prohibit user IDs and passwords from being shared.	X	X
10.1	Encryption		
10.1.1	Encrypt transmissions of Client Personal Data between the parties using a minimum of 128-bit encryption.	X	X
10.1.2	Mobile phones and tablets will be protected via a mandatory PIN, restrictions on amount of email that can be stored on the device, and a remote wipe capability.	X	
10.1.3	Full hard disk encryption at a minimum of 256-bit encryption on all workstations in use to deliver Services (i.e. Accenture, rental, client, subcontractor workstations).	X	X
11	Information Security Incident Management		
11.1	Security Incident Reporting		
11.1.1	Promptly report to an Accenture centralized management response center any actual or potential security incident that has resulted, or could be reasonably suspected to have resulted, in the loss, misuse or unauthorized acquisition of any Client Personal Data. (e.g., a lost or stolen laptop).	X	
11.1.2	Identify any additional security incident notification requirements arising from the Agreement and communicate those requirements to project personnel.	X	X
12	Compliance		
12.1	Compliance with Legal Requirements		
12.1.1	Not use Client Personal Data for any other purpose beyond provision of the contracted services, or as required by applicable law.	X	

12.1.2	For each covered statement of work, identify business, operational, and technical requirements that flow from data privacy laws that Client is subject to as part of the business process design and/or requirements definition.		X
12.1.3	Comply with controls arising out of applicable data privacy laws as they apply to Accenture as a service provider.	X	