

DIR-DCS-SCP-MSA-003

**Appendix 6 to
Eleventh Amendment of
Master Services Agreement**

August 22, 2016

Contract change log			
CCR	Amendment	Date	Description
XXXX	Amendment 11	06/15/2016	* Updated 5.0 Assessment Procedures



**Attachment to Data Center Services
Service Component Provider
Master Services Agreement**

DIR Contract No. DIR-DCS-SCP-MSA-003

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

Xerox Corporation

**Attachment 17-C
Security Assessments**

June 15, 2016

TABLE OF CONTENTS

1. INTRODUCTION.....	5
2. ASSESSMENTS.....	5
3. SECURITY ASSESSMENT COMPANY.....	5
4. ASSESSMENT COSTS	5
5. ASSESSMENT PROCEDURES.....	6
6. GENERAL AGREEMENT OF COOPERATION.....	6
7. ASSESSMENT METRICS.....	7

1. INTRODUCTION

This Attachment describes the procedures related to performing the security program assessments described in Section 3 to **Exhibit 17**. Service Provider shall observe and comply with the procedures set forth in this Attachment.

2. ASSESSMENTS

As a part of the Services, the MSI, with active participation from the Service Component Providers, shall develop, implement and maintain a continuous security program, which will comprise, without limitation, on-going activities that accomplish the goals for security management and coordinates the activities of DIR, DIR Customers, other Service Component Providers and designated Third Party Vendors (the “**Security Program**”).

DIR may conduct security assessments, including conducting monitoring and testing security programs (e.g. Controlled Penetration Tests), conducting risk assessments and performing Security Design Reviews, (the “**Assessment(s)**”) of all or any portion of the Services in order to evaluate such Security Program and determine whether the Security Program meets or exceeds the Standard of Due Care.

Without limiting the foregoing, each Assessment will examine network deployment and infrastructure to ensure the proper protection of both the Systems and data while in storage or transmission. At a minimum, each Assessment will address the following potential deployment and infrastructure issues to insure the integrity, confidentiality and privacy of data stored or transmitted by Service Provider:

- Network secure communications
- Deployment topology and internal firewalls (e.g. server authentication, distributed transactions)
- Deployment topology and remote application servers
- Infrastructure security restrictions (e.g. sensitive account privileges)
- Web farm issues (e.g. machine-specific encryption keys, authentication, or protected view state, Secure Sockets Layer, Trust levels for the target environment)

3. SECURITY ASSESSMENT COMPANY

Assessments of the Security Program may be conducted by DIR or, at DIR’s sole discretion, a third party security assessment service provider (the “**Security Assessment Company**”). Any Security Assessment Company engaged by DIR shall be an industry-recognized security assessment service provider and shall: (a) be independent; (b) have demonstrable experience in performing security assessments that are the same as or substantially similar to the Assessments; and (c) execute a non-disclosure agreement. DCS Service Providers recognize that DIR must comply with applicable Laws respecting procurement of services in connection with any engagement of a Security Assessment Company. To the extent permissible under such Laws and the reasonable practice of DIR, DIR shall consult with all DCS Service Providers with respect to the Security Assessment Company and appropriate criteria related thereto (including general terms of engagement) in making its selection; provided, however, DIR reserves the right to determine, in its sole discretion, the appropriate Security Assessment Company to be engaged and the arrangement for such engagement.

4. ASSESSMENT COSTS

Except as provided in Section 5 below, the Service Provider will be financially responsible as designated in **Attachment 4-B**.

5. ASSESSMENT PROCEDURES

The MSI will meet with DIR and/or the Security Assessment Company, as applicable, for the purpose of agreeing upon a detailed plan (including time deadlines for provision of data by all DCS Service Providers) for conducting and completing each Assessment. The MSI or the Security Assessment Company, as applicable, will “normalize” all data to obtain relevant comparisons for purposes of each Assessment in accordance with DIR’s and the State’s then-current practices and methodologies.

Service Provider shall cooperate fully with DIR and/or the Security Assessment Company and shall provide reasonable access to any premises, equipment, personnel or documents and provide any assistance required by DIR and/or the Security Assessment Company to conduct the Assessment, all at Service Provider’s cost and expense; provided, however, DIR and the Security Assessment Company shall not have access to Service Provider proprietary information where it is not relevant to the Assessment, and shall further not have access to confidential or proprietary information of other customers of Service Provider than DIR Customers. Under no circumstances will Service Provider attempt to persuade or control or otherwise influence the Security Assessment Company in the determination of its findings. The Assessment shall be conducted so as not to unreasonably disrupt Service Provider’s operations under this Agreement.

Within fifteen (15) days of an Assessment Notice Date, DIR and all DCS Service Providers will meet to jointly review the relevant Assessment report. If such report concludes that the Security Program does not meet or exceed the Standard of Due Care, then within thirty (30) days after the applicable Assessment Notice Date, the affected DCS Service Providers and the MSI shall develop and agree upon an action plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and/or recommendations identified in such report, consistent with the affected DCS Service Provider’s obligations as set forth in the Agreement. The affected DCS Service Provider shall, within six (6) months after the applicable Assessment findings have been published, complete all remedial action on critical findings or have a Third Party Assessment roadmap or a long-range project plan in place as approved by DIR in order to resolve such deficiencies, vulnerabilities and concerns and implement such recommendations.

DIR will receive Deliverable Credits pursuant to Attachment 3-C should a DCS Service Provider fail to take remedial action in accordance with such action plan.

6. GENERAL AGREEMENT OF COOPERATION

The Parties acknowledge that the procedures described in this Attachment will require further definition and clarification by the Parties. The Parties shall cooperate with the utmost good faith to reach reasonable and timely agreements on such further definition and clarification, and agree that such further definitions and clarifications shall in all respects be consistent with the terms of this Attachment. In addition, to the extent that a Security Assessment Company reasonably establishes that certain definitions, procedures and methodologies are widely used in security assessments, the Parties agree to generally rely on the Security Assessment Company’s definitions, procedures and methodologies for guidance in reaching agreement. The Parties acknowledge that in reaching the final results of an Assessment, the Security Assessment Company will be required to exercise its professional judgment and discretion in certain matters and, assuming such judgments are within established industry practices for security assessments, the Parties will defer to the conclusions of the Security Assessment Company.

Service Provider acknowledges that DIR views the right to conduct Assessments pursuant to the terms of this Attachment as a critical inducement to DIR’s agreement to many of the terms of this Agreement, including the Term and termination rights provided for in the Agreement, and therefore Service Provider agrees that it will cooperate in good faith to accomplish the objectives contemplated by this Attachment for the benefit of DIR.

7. ASSESSMENT METRICS

Service Provider will be apprised of the metrics sufficiently in advance of each Assessment to establish administrative processes to capture the necessary metric data. The exact metrics to be included in an Assessment will be contingent upon (1) the detail in which the Security Assessment Company maintains security data within its database and (2) Service Provider's ability to capture security information at the desired level of detail. DIR and the Security Assessment Companies shall use the then current ISO 27001/27002 and TAC Section 202 frameworks, where applicable, to conduct Assessments.