MANAGED SECURITY SERVICES TERMS AND CONDITIONS

This agreement is part of and incorporated within the Interagency/Interlocal Contract ("Contract") that has been entered into by the contracting parties. DIR Customer acknowledges and agrees that this Contract is with DIR and, therefore, DIR Customer does not have privity of contract with the SCPs.

Capitalized terms not defined herein shall have the meaning set forth in the relevant DIR Shared Services Contract.

DIR Customer agrees to the following conditions for receiving Managed Security Services:

1. Conditions for Providing Security Services

1.1 Access

DIR and/or Service Component Provider (SCP) shall use the Internet for primary access to DIR Customer's systems unless otherwise noted and agreed upon. DIR Customer shall not employ special access restrictions against DIR and/or Service Component Provider that it does not apply to the rest of the public network over the course of regular business.

1.2 Network Control

DIR Customer must inform DIR if DIR Customer does not control its network access and/or its Internet service is provided via a third party. DIR Customer is responsible for obtaining all necessary approvals. DIR Customer shall provide all necessary contact information for the third parties that control its network access, Internet service, and/or web applications. DIR Customer's emergency contact list shall include primary and secondary staff capable of administering DIR Customer computer systems specific to the type of services being requested or required.

1.3 Disclosure of Objectionable Material

In conducting the services authorized by DIR Customer, DIR may inadvertently uncover obscene, excessively violent, harassing, or otherwise objectionable material that may violate State or Federal law, including material that may infringe the intellectual property of a third party on DIR Customer devices or networks. DIR shall notify DIR Customer's Executive Director or highest level executive of the existence of all such objectionable and/or potentially illicit material so that DIR Customer may deal with the objectionable and/or potentially illicit material as it deems appropriate.

If DIR accesses child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110, in conducting approved Services, DIR shall report such to DIR Customer's Executive Director or highest level executive and an appropriate law enforcement agency and provide the law enforcement agency access to the visual depictions of child pornography.

If DIR accesses information that they perceive as a serious threat to human life or safety in conducting the approved Services, DIR shall report such threat to an appropriate law enforcement agency and DIR Customer's Executive Director or highest-level executive.

1.4 No Warranties and Limitation of Liability

DIR makes no representation or warranty that its security services will disclose, identify, or prevent all vulnerabilities. DIR hereby disclaims all warranties, both express and implied, including without limitation, the implied warranties of merchantability and fitness for a particular purpose. In no event shall DIR be liable for damages of any kind or nature that may arise from the services provided by DIR or DIR's Service Component Provider or Service Provider.

1.5 Service Interruption

DIR will endeavor not to disrupt DIR Customer's services and to adhere to best practices for all work performed. However, tools or services may affect the serviceability of poorly configured or overextended systems or services. It is possible that control of DIR Customer's system may be lost. For any testing that DIR may be conducting, DIR endeavors to use the safest methods to compromise DIR Customer's systems; however, DIR Customer should be prepared to restore a damaged system from a recent, acceptable backup within an acceptable time as determined by DIR Customer. During any testing DIR may conduct, DIR will NOT conduct any deliberate Denial-of-Service attack. DIR Customer agrees not to hold DIR liable in the event of any service interruption(s) that may arise as a result of performance of any Services. If either party becomes aware of a service interruption, that party will notify the other party's emergency contact.

1.6 Termination of Services

If DIR Customer terminates certain Services, that it requested and approved, for convenience, DIR Customer shall pay the remaining requisite unrecovered costs that have already been incurred prior to the notice of termination, such unrecovered costs will be calculated in accordance with the relevant DIR Shared Services Contract, SMM, or other DIR Customer approved terms. DIR Customer understands that it may not be able to terminate services or receive any refund of a pre-payment after approving the relevant financial solution.

2. DIR and DIR Customer Responsibilities

2.1 DIR Customer agrees as follows to the extent assessment Services are requested or required:

a) DIR Customer responses to information requests and artifacts gathering pertinent to this security and risk assessment will be timely;

b) The artifacts data are reasonably available via interviews and documents review;

c) DIR Customer will make available the necessary Subject Matter Expert (SME) with required expertise to work with the SCP Assessment Team and will remain available thru the duration of the assessment;

d) DIR Customer SME will be available when required for interaction with the SCP Assessment Team and that all the interviews will be conducted over the number of consecutive days as established during the project planning and scheduling phase;

e) DIR Customer is responsible for the coordination and scheduling of resources and providing meeting facilities as necessary;

f) Deliverables will be complete when DIR Customer has approved in writing that the deliverable meets the acceptance criteria;

g) All document deliverables must be in formats (hard copy and/or electronic) as specified by DIR Customer. At a minimum, the formats must be in industry-accepted standards (e.g., MS Word, MS PowerPoint MS Project);

h) DIR Customer will assist with meeting coordination for meetings between DIR Customer Key Personnel and DIR and the Service Provider and other staff to gather requirements and other activities;

i) DIR may receive final copies of reports if DIR is paying for the assessment.

2.2 Penetration Testing

2.2.1 DIR Customer agrees as follows to the extent penetration testing ("PT") is requested or required:

a) SCP may conduct a passive scan to determine the number of live IPs within the Customer designated IP range.
b) DIR Customer shall not intentionally place an unsecured system or device in the test scope.
c) If DIR Customer detects SCP testing activities, DIR Customer technical staff shall follow standard operating procedures and policies.

2.3 DIR Customer Compliance

DIR Customer shall comply with all policies, procedures, and processes in the relevant SMM(s) and as provided by DIR.