The Power of Information

Access to billions of records, to locate
the exact data when you need it.

Enformion Product Specifications

FOR PUBLIC SECTOR
SINs 518210C, 511210

Confi-Chek

Table of Contents

"When it comes to quality data on a budget, it's the best of both worlds"

- A Recent Data Customer

Contact Information

Contact Information

Schedule Title
Information Technology (Cloud Solutions)

Contract Number
47QTCA19D001T

Contract Period
Nov. 2, 2018, through Nov. 1, 2023

Contractor
Confi-Chek, Inc.
1821 Q Street
Sacramento, CA 95811

Website
https://www.confi-chek.com

Contact
Scott Johnson
Director of Government Services

Telephone
(855) 281-3915

Fax
(916) 790-5891

Email
publicsector@enformion.com

DUNS Number
859038655

CAGE Code
4DBU1

Tax Identification Number
94-3359257

Primary NAICS 519130
Online Information Services, Small Business

Secondary NAICS 518000
Data Processing, Hosting, Related Services, Small Business

Contractor Summary

Awarded Special Item Numbers
SIN 518210C
SIN 511210
NAICS 519130 - On-Line Information Services, Small Business
Secondary NAICS 518000 - Data Processing, Hosting, Related Services, Small Business

Pricing
Please see individual product descriptions and associated pricing tables.

Maximum Order
$500,000

Minimum Order
$100

Lowest Priced Models
Enformion for Contact Tracing $40.30
SIN 511210 **MODEL** 005-WEB-0001

GSA Enformion Monthly $0.00
SIN 518210C **MODEL** GSA-Monthly-ZERO

Geographic Coverage
Confi-Chek provides services in all CONUS and OCONUS locations.

Point of Production
1821 Q Street, Sacramento, California 95811, USA

Discounts
Pricing contained herein includes negotiated discounts.

Volume Discounts
Varies for products and quantities ordered.

Payment Terms
Net 30

Information for Ordering Offices
No prompt payment discounts are available or offered.

Notification that Government purchase cards are accepted
Yes.

Government purchase cards are accepted or not accepted above the micro-purchase threshold
Yes.

Items Produced Outside the United States
None.

Time of Delivery
Negotiated per agency request.

Expedited Delivery
Negotiated per agency request.

Overnight Delivery
Negotiated per agency request.

Urgent Requirements
Negotiated per agency request.

FOB Points
Varies by services ordered.

Ordering Address
See contractor address.

Registration In CCR Database
Registered in SAM database.

Section 508 Compliance
Yes.

Warranty Terms
Standard

Confi-Chek

About Confi-Chek, Inc.

Founded in 2000, Confi-Chek, Inc. is a leader in the Data-as-a-Service industry. Confi-Chek's public and proprietary data sources provide data and intelligence to government and commercial organizations, with more than 6,000 data sources and 43 billion records.

Built on next-generation technology and data solutions, Confi-Chek provides powerful search technology and best-in-class innovation to deliver billions of records via the Enformion investigative web platform, API, and batch processing.

Confi-Chek partners with customers to deliver data solutions customized to their workflow. Sustaining key, long-standing strategic partnerships with a customer-centric approach, Confi-Chek offers best-of-breed data, analytics, and applications to our customers seeking insights to enhance knowledge, improve efficiencies, and better serve their clients and constituents.

The big data platform connects billions of records to build comprehensive profiles about individuals in the United States. Confi-Chek's significant data breadth consists of consumers in credit, under-banked, property records, and utility files, and more. Data includes individuals not typically found in regular credit and consumer databases, including those with limited or no credit histories. The data is matched to public records data sets, including bankruptcies, liens, criminal records, evictions, foreclosures, business data, and more.

Confi-Chek has its roots in the investigation and person locator services industry, providing data to a variety of industries, including law enforcement, investigative, debt collection, and financial services. Additional market offerings include witness locator services for law firms, tools for the detection and investigation of fraudulent activity, constituent communications, and augmentation of law enforcement and private investigator's information systems. Confi-Chek's consumer business is established as the well-known Internet brand, PeopleFinders.com, and continues to enjoy strong commercial success.

Confi-Chek employs best-in-class information and cybersecurity practices, including next-generation firewall systems, minimum access network provisioning for employees, and multi-factor authentication to internal corporate policies and resources.

The Enformion Investigative Web Platform

Confi-Chek offers the Enformion investigative web portal on the GSA Schedule 70 contract with transactional and flat-rate pricing options.

Web Application Portal

Confi-Chek offers the Enformion investigative web portal on the GSA Schedule 70 contract with five flat-rate and two transactional subscription pricing models. Data access via Application Program Interface (API) and Batch File Exchange (Batch) is available with any subscription selection, in addition to the web application portal.

The data content for each subscription pricing model is identical. The pricing alternatives serve different anticipated usage volumes, customer needs, and budget.

Pricing discounts are offered and quoted based on the volume and length of the subscription.

Data Resources

The following are descriptions of the various Core Resources and available Add-On Resources. Data and reports are searchable by multiple inputs, including name, address, phone number, SSN, DOB, and more.

Core Resources

Premium People Search
With coverage of over 95% of US Population, includes current and 40-year historical addresses, emails, phone numbers, relatives, associates, and SSNs, DoBs.

Comprehensive Person Report
Person addresses, AKA's, aircraft, arrests, assessor, bankruptcies, birth, criminal, DBA/FBN, DEA licenses, death, deeds, divorce, email addresses, evictions, foreclosures, judgments, liens, neighbors, phone numbers, professional licenses, relatives/associates, nationwide criminal, traffic, US corporations.

Vehicle (Aircraft, Auto, Vessel) Reports
Registered aircraft/vehicles/vessels, searchable by the owner, address of registration record, SSN, or registry tag number with variances by individual state regulation.

Property Records
All current and previous real property owned, with assessor and deed records for each, including valuation models; more than 3,000 counties covered nationwide.

US Corporate Filing Records
Executives, affiliated businesses, corporate bankruptcies, status of their corporate filings and annual disclosures, DBAs, and more. Liens and UCC filings are also available and included if relevant.

UCC Filings & Liens
Covers nationwide UCC filings and UCC liens with identified companies, business owners, financial scores, and more. More than 38MM records added monthly.

Reverse Phone Lookup
Instantly locate owners of phone numbers, including mobile, landline, VOIP, with more than 600MM phone numbers.

Public Records Search
Comprehensive details based on publicly available records, including bankruptcy, liens, judgments, criminal records, evictions, foreclosures, property records, and more. This search is included in a Comprehensive Person Report.

Criminal Record - Nationwide
Nationwide arrests, criminal convictions, sex offender, traffic, and wants & warrants, OFAC; more than 600MM offense and offender records.

SSN Verification
History of all individuals with a provided Social Security Number associated with the record.

Corporate Records – New Business Records
Franchise relationships, and other affiliated links such as common registration agents or officers.

Professional Licenses
A unique data set of aggregated professional board-issued licenses.

DEA Licenses
Drug Enforcement Administration (DEA) license and the registration number issued to a health care provider allowing the provisioning of prescriptions for controlled substances.

Identity Verification
Using PII data, users can instantly verify identity and score accuracy using names, address, phone number, SSN, DOB.

Bankruptcy Records
Access more than 32 million bankruptcy records and covering 50 states with details including case number, chapter type, disposition, assets, attorney names, courts, debtors, and more.

Judgments
With more than 100M records in the U.S., judgment include records for all 50 states with debtor records, total lien/judgment data.

Eviction Records
Eviction records cover all 50 states, with details related to each eviction record.

Patriot Act
Patriot Act list statuses.

Workplace: People at Work
Locate a person's employment history with self-reported records, including company name, address, dates, and historical records.

Liens
Involuntary liens include tax liens with more than 90 million records. Details include access to more information associated with each lien, petitioner, respondent, tax lien dates, and more.

Pre-Foreclosure Records
Pre-foreclosure records include nationwide coverage with details of dates, names, loan amounts, defaults, and more.

Relatives and Associates
Locate relatives and associates with 40 years of address and telephone number histories, including shared residences.

Deceased Records
With more than 100M deceased records, data is updated regularly and flagged to the unique person records with date of death.

Add-On Resources

Social Media Report
An exhaustive search of an individual's social media accounts, records, postings and "footprints" around the web.

Real-Time Incarceration Records
Access to real-time incarceration data available on the Enformion investigative web platform.

Data Alerts and Monitoring
Continuous monitoring of persons of interest can be added with alerts highlighted when records change, and when new records are added.

Vehicle Registration Records
Single-state search of an individual's driver record; fees vary by state.

Comprehensive Business Credit Reports
Access to comprehensive business credit reports available on the Enformion investigative web platform.

Custom Data Products
Custom integration of Confi-Chek and third-party data.

Risk Indicators

With each record searched and presented either via the online investigative platform, API or batch, flags are set to identify derogatory indicators as well as asset integrators, including:

- Bankruptcies
- Liens
- Judgments
- Criminal Records
- Evictions
- Foreclosures
- Property Ownership
- Professional Licenses
- Driver's License Number
- Workplace Data
- Business Records

Enformion for Fraud and Case Investigations (EFCI)

The EFCI Suite offers four pre-bundled packages to choose from, each with flat-rate subscription pricing.

Enformion for Fraud and Case Investigations equips civilian, government, and armed services professionals with the tools and data they need to:

- Locate people
- Investigate individuals
- Uncover assets
- Investigate businesses
- Detect fraud
- Uncover associate linkages between people and businesses

The platform streamlines investigative processes to improve efficiency. Four pre-configured solutions are offered, as well as the customizable and flexible Enformion Enterprise package, for unique requirements.

These packages include:

- **Enformion for Credentialing (EFC)**
  Verify Identities and Mitigate Risk
- **Enformion for Civil Enforcement (ECE)**
  Reduce Entitlement Program Fraud and Waste
- **Enformion for Justice (EFJ)**
  Investigate Leads, Cases, and Persons of Interest
- **Enformion for Contact Tracing (ECT)**
  Locate Individuals Possibly Exposed to a Contagious Disease
- **Enformion for Enterprise (EE)**
  Customizable Solutions to Meet a Wide Variety of Business Requirements

Enformion for Credentialing (EFC)

Government customers require accurate identity verification and risk indicators to make efficient identity and credentialing adjudicative decisions.

EFC provides agencies specialized data to verify individuals' identity and risk indicators before the issuance of access credentials. Identity Verification is included in the EFC product suite.

In the past, such investigations required manual research and verifications to organize the relevant facts of the subject's history to render a decision. Enformion accelerates credentialing examinations with accurate data you can trust. Our data will help to speed up the verification process, as well as ensure authorized individuals' expedient access.

With EFC, access is provisioned to Enformion's comprehensive Premium People Search, with Identity Verification and risk indicator data. EFC services can also be accessed via API integration and batch processing.

What's Included:

Base Contact Information:

- Current address
- Phone numbers (mobile, landline, VOIP)
- Email addresses
- AKAs
- SSN verification
- DOB verification
- Identity Verification

Comprehensive Data Attributes:

- Bankruptcies
- Liens
- Judgments
- Foreclosures
- Evictions
- Nationwide criminal records
- Property ownership

Available Data Access:

- A web platform for manual searches with seat pricing
- Customized Batch Processing for high-volume demands
- API access services for integration with third-party identity verification applications

Enformion for Civil Enforcement (ECE)

ECE serves the needs of government agencies that investigate or adjudicate claims for entitlements, benefits, welfare programs, or environmental regulations.

Government subsidies, welfare, health, and other benefits programs are there to help those in need. Reducing fraud and waste is a critical part of maintaining program integrity.

The data available through ECE is invaluable to those that deal with entitlement fraud and waste as it relates to social benefits, including:

- Pension and retirement
- Health & Human Services
- Healthcare benefits
- Unemployment claims
- Environmental enforcement
- Tax & Revenue
- Provider claims fraud
- Medicaid dual enrollment
- Women, Infants, and Children (WIC) vendor adjudication
- Pretrial discovery

ECE can help detect the incidence of fraud and waste more quickly than traditional modes of investigation, with instant access to premium data.

What's Included:

Base Contact Information:

- Current address
- Phone numbers (mobile, landline, VOIP)
- Known relatives and associates
- AKAs
- Property ownership and records
- Business and place of employment records

Comprehensive Data Attributes:

- Bankruptcies
- Liens
- Judgments
- Foreclosures
- Evictions
- Nationwide criminal records

Available Data Access:

- A web platform for manual searches with seat pricing
- Customized Batch Processing for high-volume demands

Enformion for Justice (EFJ)

EFJ provides criminal justice and national security agencies with quick access to the investigative tools and resources they need to locate persons of interest and develop investigatory leads.

The software, tools, and data bundled in EFJ can benefit users like:

- Departments of Justice
- State prosecutors
- Tax courts
- State police
- Public Safety offices
- Correctional institutions
- Armed Services
- Homeland Security
- Private sector legal defense
- Emergency management

With ease of use and instantaneous data retrieval, EFJ pinpoints a person's contact information, last known residence, personal relationships, business entanglements, tangible assets, and contextual information found via social media searches and data retrieval.

What's Included:

Base Contact Information:

- Current address, with 40-year historical data
- Phone numbers (mobile, landline, VOIP)
- Known relatives and associates
- Email addresses
- AKAs
- Property ownership and records
- Workplace: place of employment records
- Professional licenses
- Business Records

Comprehensive Data Attributes:

- Bankruptcies
- Liens
- Judgments
- Foreclosures
- Evictions
- Nationwide criminal records
- Real-Time Incarceration Search Packs
- Social Media Records Packs
- UCC Filings & Liens

Available Data Access:

- A web platform for manual searches with seat pricing
- Customized Batch Processing for high-volume demands

Enformion for Contact Tracing (ECT)

ECT provides an immediate starting point for public health and disaster relief workers to quickly identify a subject's network of family, friends, neighbors, and work associates.

When a victim presents with a highly contagious disease, such as COVID-19, public health workers must act quickly to identify the other individuals with whom the subject has been in recent contact. Beginning by identifying friends, family members, and close neighbors is critical for effective contact tracing.

Enformion combines personal relationship information with skip-tracing data to quickly reach those potentially affected individuals.

And with support for in-office researchers and field workers alike, the Enformion platform is compatible with all major desktop web browsers and mobile devices.

What's Included:

Base Contact Information:

- Current address/location
- Current phone numbers – mobile and landline
- Known relatives and associates
- Place of work information
- Neighbor information

Comprehensive Data Attributes:

[not included in package]

Available Data Access:

- A web platform for manual searches with seat pricing
- Customized Batch Processing for high-volume demands

Enformion for Enterprise (EE)

EE combines unlimited core data services with the flexibility to add additional databases or features. Confi-Chek offers our Enformion Enterprise package as a starting point for customized service delivery to meet customer requirements for unique combinations of search and database access features.

And with support for in-office researchers and field workers alike, the Enformion platform is compatible with all major desktop web browsers and mobile devices and includes comprehensive data, covering more than 95% of the U.S. population.

What's Included:

Base Contact Information:

- Current address
- Phone numbers (mobile, landline, VOIP)
- Known relatives and associates
- AKAs
- Property ownership and records
- Business and place of employment records

Comprehensive Data Attributes:

- Bankruptcies
- Liens
- Judgments
- Foreclosures
- Evictions
- Nationwide criminal records

Available Data Access:

- A web platform for manual searches with seat pricing
- Customized Batch Processing for high-volume demands

Part Number	Product Name	GSA SIN	Monthly Price Per Seat, Including IFF
002-WEB-0001	Enformion for Credentialing	511210	$50.38
003-WEB-0001	Enformion for Civil Enforcement	511210	$61.46
004-WEB-0001	Enformion for Justice	511210	$109.82
005-WEB-0001	Enformion for Contact Tracing	511210	$40.30
001-WEB-0001	Enformion for Enterprise	511210	$72.54

GSA Pricing Schedule

Enformion transactional access is offered for interactive data discovery, data mining, and reporting. API and batch file access options are also available with volume-based discounting.

Web Application Portal

Our Enformion investigative web portal (Enformion online platform) subscription is offered with two transactional pricing models. The data content for each subscription pricing model is identical.

The **GSA Monthly Zero** features our base GSA-negotiated query and reporting in-app usage fees but does not have a monthly minimum fee.

The **GSA Monthly 25** includes a sizable discount for each in-app query and reporting fee for a $25.00 monthly commitment per seat. The $25.00 monthly fee is credited to in-app usage incurred monthly; any surplus does not roll over to the following month.

Part Number	Product Name	GSA SIN	Monthly Price Per Seat, Including IFF
GSA-Monthly-25	GSA Enformion Monthly	518210C	$25.19, Subject to In-App Additional Pricing
GSA-Monthly-ZERO	GSA Enformion Monthly	518210C	$0.00, Subject to In-App Additional Pricing

In-App Service Delivery Pricing (GSA Monthly Zero and Monthly 25 Only)

Service	Description	GSA Monthly Zero	GSA Monthly 25
Comprehensive Person Report	A comprehensive Background Report including person details, bankruptcies, liens, judgments, criminal records, evictions, property records, pre-foreclosure, business records, deceased records	$3.48	$3.17
Premium Person Search	Current Locator and Contact Information Report including full names, addresses, phones, emails relatives, associates, DOB, and SSN	$0.70	$0.63
Real Property-Combined Search	Comprehensive Report for a Provided Property Address or APN including mortgage, open liens, property values and more	$1.39	$1.27
Assessor Property Records	County Assessor Data	$1.39	$1.27
Deeds Records	Records of Property Deeds records	$1.39	$1.27
SSN Verifier Plus	Verifies Social Security Number Provided	$0.17	$0.16
Bankruptcy, Lien, Judgement Records - combined	Comprehensive Debt Records including details Bankruptcy, Liens, Judgements records	$2.09	$1.90
Bankruptcy Records	Filing and Discharge Dates of Bankruptcy	$0.70	$0.63
Eviction Records	Nationwide Eviction Case Records	$0.70	$0.63
Pre-Foreclosure Records	Real Property Pre-Foreclosure Records	$0.70	$0.63
Tax Lien Records	Unpaid tax lien information	$0.70	$0.63
Civil Judgments	Civil Case Judgment Records	$0.70	$0.63
Criminal Records	State/Local/Federal Criminal Records including felonies, misdemeanors, wants, warrants, sex offender, OFAC/blacklist, warrants, arrests	$3.48	$3.17
Arrest Records	State/Local/Federal Arrest Records	$0.70	$0.63
Prohibited Party / Terrorism Search (OFAC)	OFAC prohibited parties list	$0.35	$0.32

Service	Description	GSA Monthly Zero	GSA Monthly 25
Traffic Records	Nationwide Traffic Records	$0.35	$0.32
National Warrants	Nationwide Criminal Wants/Warrants	$0.35	$0.32
Criminal Profile	Comprehensive Criminal Record Report	$5.21	$4.76
Combined Business Search	Comprehensive business reports from US Corporations, new business filings and UCC filings	$2.09	$1.90
DBA / FBN Records	New business filings database including Corporate and business Doing Business As (DBA) and Fictitious Business Names (FBN)	$0.70	$0.63
FEIN-Tax ID Records	Federal Employer ID Records	$0.70	$0.63
U.S. Corporation Records	US Corporation Registration sources from Secretary of State filings	$0.70	$0.63
Workplace Records	Place of Employment Records, self-reported	$1.74	$1.59
Social Media Search	Real-time Internet search additional social media profiles, and related website content	$6.95	$6.88
Mini Profile	Person Profile report	$1.04	$0.95
Neighborhood Profile	Search by address to return Neighbors	$0.70	$0.63
Shared Residence Report	Identification of Shared Residence Address of Individuals	$0.70	$0.63
DEA Licenses	DEA Controlled Substance Licenses	$0.70	$0.63
Hunting & Fishing Licenses	Hunting and Fishing License Holders	$0.35	$0.32
Pilot's Licenses	FAA Pilot's Licenses	$0.70	$0.63
Professional Licenses	State Professional License Issue	$0.70	$0.63
All Docket	All Court Docket Records	$2.78	$2.54
Appellate Docket	US Appeals Court Docket	$0.70	$0.63
Bankruptcy Docket	US Bankruptcy Court Docket	$1.39	$1.27
Federal Civil Docket	US Civil Case Docket	$1.39	$1.27
Federal Criminal Docket	US Federal Criminal Record	$1.39	$1.27
Sex Offender Records	National Sex Offender Registry	$0.35	$0.32
Birth Records	Stand-alone search of birth records	$0.35	$0.32
Death Records	Stand-alone search of deceased records	$0.17	$0.16
Divorce Records	Stand-alone search of divorce records	$0.35	$0.32
Marriage Records	Stand-alone search of marriage records	$0.17	$0.16
Premium Profile Report	Premium Person Profile Record	$3.48	$3.17
Telephone / Cell Phone Report	Nationwide Landline and Mobile Phone Numbers for the Subject	$2.09	$1.90
Aircraft Records	Aircraft Registration	$0.70	$0.63
Domain Registrations	Internet Domain Name Registrations	$0.35	$0.32
Vehicle Ownerships	Motor Vehicle Ownership records	$1.39	$1.27
Vessel Records	Vessel Registration Information	$0.70	$0.63

Available Add-Ons

Confi-Chek offers search and reporting of our Core Resources to our government customers on an unlimited basis, at no additional cost.

Core Resources are defined as those capabilities that we provide for shared access by the majority of our customers. Confi-Chek integrates additional specialized capabilities our partners, on an on-demand basis. (See "Data Resources," pages 5, for more information.)

Real-Time Arrest and Incarceration Search

A real-time search for a subject's recent arrest, booking, and incarceration throughout approximately 87% of US jurisdictions, in real-time. The recency of available data will range from a few hours to one business day, dependent upon sourcing input lag.

Comprehensive Business Credit Report

Confi-Chek has partnered with an expert in the business financial reporting market to provide integrated analytical reporting of the subject company's economic outlook.

Publicly traded and privately held company reports are available, with varying levels of information available. Data such as import/export trade volume, quick ratios, average days-to-pay vendors, and other descriptors with the provided financial reporting suite.

Premium Social Media Search

Profiles include a basic social media profile summary, such as known usernames associated with the subject. The Premium Social Media Search conducts an exhaustive search of the subject throughout social media and the broader Internet.

Reports provide a thumbnail images and a hyperlink to the source. Telephone numbers, family members, and business references (such as social media reviews like those on Yelp of a business owned) are common. Or, a business search can be performed using criteria like the business name or a published business phone number.

Continuous Monitoring

Persons of Interest may be monitored for future updated information, such as a newly activated mobile phone or a freshly reported address. Records can be set up to monitor for changes include:

- Bankruptcies
- Liens
- Judgments
- Criminal Records
- Evictions
- Foreclosures
- Property Ownership
- New Addresses
- New Phone Numbers

Available Add-On Pricing Schedule

Part Number	Product Name	Quantity	GSA SIN	Price, Including IFF
005-MTR-4001	Continuous Monitoring Service	1	511210	$0.14
005-MTR-4002	Continuous Monitoring Service	100	511210	$13.50
005-MTR-4003	Continuous Monitoring Service	1,000	511210	$127.90
005-WEB-0009	Premium Social Media Report	100	511210	$593.81
005-WEB-0010	Premium Social Media Report	1,000	511210	$5,938.08
005-WEB-0012	Real-Time Arrest and Incarceration Search	1,000	511210	$1,141.94
005-WEB-0013	Real-Time Arrest and Incarceration Search	100	511210	$114.19
005-WEB-0054	Comprehensive Business Credit Report	100	511210	$3,654.20

API and Batch File Services

Core data assets can be delivered via API web services or as a downloadable file drop for use in third-party software applications (such as case management systems). To provision, Confi-Chek provides security credentials in the form of encryption keys with request file templates.

These services are offered in conjunction with flat-rate web seat subscription options.

End-User Support

The data provider industry for the public sector is becoming increasingly specialized. That's why Confi-Chek provides much more than just exceptional data. The following are the additional services we offer to meet the needs of our customers and their unique mission requirements.

End-User Support and Training

Confi-Chek provides end-user training seminars at no cost as part of the Enformion investigative web platform on-boarding process. End-user support, such as search assistance and technical support, are provided with no charge to government customers. Several calendar events are provided during the on-boarding process over a variety of days and times, ensuring availability for all interested customer staff to attend.

The end-user training demonstrates the significant features of the platform, performing basic database searches and reporting, investigative techniques, and recommendations to maximize search results with a minimum amount of effort.

Additional training can be provided periodically, intended to assist our customers with introducing newly hired staff members to the Enformion platform.

Confi-Chek's call center and account management team provide investigative support for customers with specific case assistance needs.

Vendor-Provided Technical Support

The Confi-Chek call center and account management team provide technical support, defect resolution, and investigative support for customers upon request.

Master Services Agreement

This Master Services Agreement (together with the Exhibits attached hereto, this "**Agreement**") is entered into between Confi-Chek, Inc. ("**CCO**"), a California corporation, having its principal place of business at 1915 21st Street, Sacramento, CA 95811, and the Ordering Activity under GSA Schedule contracts identified in the Purchase Order, Statement of Work, or similar document ("**Customer**" or "Ordering Activity. The Master Services Agreement, together with Exhibits A, B and C is effective as of the effective date stated in the Purchase Order, Statement of Work, or similar document (the "Effective Date"). CCO and Customer may execute one or more Exhibit As hereunder and each Exhibit A is subject to the terms of this Agreement.

The parties agree as follows:

1. **CERTAIN DEFINITIONS**. The following definitions apply for purposes of this Agreement:
"CCO API" means an application programming interface provided by CCO to Customer that allows Customer to submit Search Requests to the CCO API.
"CCO Data" means data that is obtained from the CCO Services or Network, and that includes all languages, editions, issues, versions, revisions, modifications, enhancements, and updates thereto during the Term of this Agreement.
"CCO Products" means CCO Services, Network, CCO API and/or CCO Data, together with any CCO Confidential Information.
"CCO Services" means the nationwide nonpublic and/or public record information, document retrieval and related services provided by CCO through the Network.
"FCRA" means the Fair Credit Reporting Act, 15 USCA § 1681, et seq., as now or hereafter amended.
"GLBA" means the Gramm-Leach-Bliley Act, 15 USC. § 6801 et seq., as now or hereafter amended.
"Network" means CCO's online data retrieval system of proprietary databases and data and information obtained from third parties.
"Permitted Uses" means the use of CCO Products in a manner strictly in accordance with purposes permitted under this Agreement and in compliance with all applicable laws and regulations.
"Search Request" means a search for CCO Data through the CCO API by Customer.
2. **SERVICES AND LICENSE.**

2.1 **Products; Purpose**. CCO provides CCO Products. Customer hereby agrees to use the CCO Products for the sole purpose as set forth in Exhibit A or the executed Purchase Order (the "Purpose").

2.3 **License.** CCO hereby grants to Customer a nonexclusive, nonassignable, nontransferable, limited license to use the CCO Products solely for the Purpose. Nothing in this Agreement is intended to or should be construed to prevent CCO from entering into similar agreements with other persons or entities regarding all or any part of the CCO Products.

2.3 **Restrictions and Limitations.** Customer warrants that:

(a) Customer will not, either directly or indirectly, itself or through any agents or third party: (i) request, compile, store, maintain or use any CCO Products to build its own database or accumulate any CCO Products or content for any other use; or (ii) copy or reproduce any portion of the CCO Products; or (iii) redistribute, disclose, market, rent, lease, solicit, supply or transfer to any third party any portion of the CCO Products; or (iv) store any results returned by the CCO Products or anything Derived therein, except to the extent necessary for purposes of audits, the Purpose or other purposes required by applicable law. "**Derived**" means data that is directly or indirectly related to the presence or absence of the CCO Data, or is based on or having its origin in CCO Data.
(b) Customer will not disassemble, decompile, or in any way reverse engineer the CCO Products.
(c) Customer will comply with the CCO policies and procedures attached to this Agreement("**Policies**").
(d) Customer will only use the CCO Products for the Purpose.
(e) Customer will not market the CCO Products under the CCO name.
(f) Customer will not distribute, provide, license, transfer, or sell the CCO Products to any third parties.
(g) Upon receipt of any updated CCO Products from CCO, Customer will promptly replace and destroy any outdated CCO Products in its possession prior to the update.
(h) Customer will not merge any CCO Data with any consumer reports as the term "**consumer report**" is defined in the FCRA.
(i) Customer will not delete, alter, disclose or otherwise modify any security codes or protocols within the CCO Products or in any way compile and/or offer for use or sale any CCO Products or other data contained therein in a form where any security codes or protocols are deleted, altered, disclosed or otherwise modified.

2.5 **Removal of Data.** From time to time, CCO may, for any reason whatsoever, suppress or remove information pertaining to one or more particular persons from the CCO Data ("**Removals**"). CCO will provide Customer with notice of all such Removals. As soon as commercially reasonable, but no later than ten (10) business days after Customer' receipt of the notice of Removals from CCO, Customer will: (a) remove or suppress such persons who are the subject of the Removals from any and all materials provided by CCO to Customer; and (b) exclude such persons who are the subject of the Removals from any CCO Data that Customer may provide in its ordinary course of business.

2.6 **Feedback.** Customer will provide comments or any other form of feedback ("Feedback") relating to the CCO Products as reasonably requested by CCO. Feedback becomes the exclusive property of CCO and is CCO Confidential Information. CCO acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

3. **COMPLIANCE WITH LAWS; SECURITY OF DATA.**

3.1 **Compliance with Laws.** Customer will not use the CCO Products in a manner contrary to or in violation of any applicable federal, state, or local law, rule, or regulation, including, but not limited to, the GLBA and the FCRA. Customer certifies that it will not use any information obtained through the CCO Products as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, for employment purposes, for governmental licenses, or for any other purpose for which one might properly obtain a consumer report, as defined by the FCRA. Customer specifically agrees that CCO Products will not be merged with consumer reports as such term is defined in the FCRA. CCO reserves the right to insert certain information (sometime referred to as seeding) into the data available from the CCO Products for the purpose of determining Customer's compliance with the terms of this Agreement.

3.2 **Privacy and Security Requirements.** Customer will comply with all applicable laws concerning the CCO Products, including without limitation applicable laws regulating how an organization manages, protects and distributes confidential information and laws restricting the collection, use, disclosure, processing and free movement of personal information (collectively, the "**Privacy Regulations**"). The Privacy Regulations include, to the extent applicable, the Federal "Privacy of Consumer Financial Information" Regulation (12 CFP Part 40) and Interagency Guidelines Establishing Information Security Standards (App B to 12 CFR Part 30), as amended from time to time, issued pursuant to the GLBA. Customer expressly agrees that it will comply with the use requirements applicable pursuant to the GLBA and similar laws, including without limitation each of the permissible use requirements set forth on Exhibit C attached hereto.

Customer will maintain all appropriate administrative, physical and technological processes and equipment to store and securely protect the CCO Products, including without limitation, maintaining an information security program that is designed to protect information processing system(s) and media containing the CCO Products from internal and external security threats, and the CCO Products from unauthorized use or disclosure. In addition and to the extent applicable, Customer specifically agrees to comply with each of the security requirements set forth on Exhibit B attached hereto. CCO may, from time to time, provide written notice to Customer of updates to the security requirements set forth on Exhibit B, and Customer will comply with the updated security requirements following a mutually agreed upon and reasonable period of time. Customer acknowledges and agrees that Customer has an ongoing obligation to protect and preserve the confidentiality, privacy, security and integrity of the CCO Products, and the standards embodied in this Agreement are merely minimum standards of conduct for Customer in furtherance of the foregoing continuing obligation.

4. **FEES, AUDIT RIGHTS, AND FINANCIAL STATEMENTS.**

4.1 **Fees.** Customer agrees to pay CCO the applicable charges as set forth in Exhibit A of this Agreement in accordance with the Purchase Order and GSA Schedule Pricelist. CCO shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3. However, Customer will not be responsible for taxes imposed upon CCO by any federal, state or local authority against the net income of CCO. Payment inquiries should be remitted in writing to the following address: CCO, 1915 21st Street, Sacramento, CA 95811, or by fax to (916) 739-1118.

4.2 **Invoicing and Payment.** Customer will pay all invoices from CCO issued pursuant to this Agreement within thirty (30) days of the invoice receipt date.

4.3 **Unpaid or Outstanding Balances.** Without limiting any of CCO's remedies for non-payment or late payment of any amounts due by Customer to CCO,

(a) amounts which are not paid within sixty (60) days of the invoice date or the date on which CCO notifies Customer, whichever is sooner, may be subject to late interest as indicated by the Prompt Payment Act (31 USC 3901 et seq) and Treasury regulations at 5 CFR 1315.

(b) Reserved.

4.4 **Audit Rights.** Customer will maintain records including, but not limited to complete and accurate accounting records in accordance with generally accepted accounting practices, to substantiate Customer's performance under this Agreement including, without limitation, Customer's compliance with payment, legal and all security requirements. Customer will preserve such records for a period of at least thirty-six (36) months after termination of this Agreement. Moreover, no more than one (1) time per calendar year during the Term of this Agreement and no more than once per calendar year after termination of this Agreement and for no more than thirty-six (36) months thereafter, CCO will have access to those records of Customer that are necessary to determine Customer's compliance with its obligations under this Agreement and subject to Government security requirements to Customer's facilities for the purpose audit either through its own employees, representatives or an independent public accounting firm selected by CCO (the "**Auditor**"). Any such review of Customer's records, facilities, or both, may be conducted during Customer's normal business hours upon CCO providing Customer no less than five (5) business days' prior written notification; provided, however, that in the event of a material breach including, but not limited to, any material deficiency in Customer's performance of this Agreement, then such interval restriction and required prior written notification, except for reasonable notice, will not apply. For each third party who provides CCO Product-related services to Customer, from time to time, CCO will have the right to review, at CCO's expense, each such third party's security processes and procedures related to the transmission, storage or processing of CCO Products. Customer will reasonably cooperate and will request each such third party to also reasonably cooperate, with CCO and any CCO requests in conjunction with all such reviews including, but not limited to CCO requests to correct any deficiencies discovered during such audits within a period of time mutually agreed upon and/or suspend any further transmission of CCO Products until such deficiencies are corrected. Customer agrees that it will reasonably cooperate with all such reasonable CCO requests for information and audits. Customer's obligations to comply, with the provisions of this Agreement are not contingent upon, or otherwise affected by, the audit rights of CCO.

5. **INTELLECTUAL PROPERTY; CONFIDENTIALITY.**

5.1 **Intellectual Property.** Customer acknowledges that CCO has expended substantial time, effort, and funds to collect, arrange, compile, create, and deliver the CCO Products. Customer agrees not to reproduce, retransmit, republish, or otherwise transfer for any commercial or other purpose any information that Customer receives from CCO or the CCO Products except as permitted under this Agreement. Customer acknowledges that CCO (and/or CCO's third-party data providers) will retain all right, title, and interest in and to the data and information provided by the CCO Products under applicable contractual, copyright, intellectual property and related laws, and Customer will use such materials consistent with CCO's interests and notify CCO of any threatened or actual infringement of CCO's rights. Customer further acknowledges and agrees that it will acquire no right, title, or interest under applicable copyright or other laws in the CCO Products and materials provided or accessed under this Agreement. Customer will not remove or obscure the copyright notice or other notices contained on materials accessed through the CCO Products. Ownership of derivative works should be as set forth in the copyright statute, 17 USC. § 103 and the FAR clause at 52.227-14, but at a minimum, the Ordering Activity shall receive unlimited rights to use such derivative works at no further cost.

5.2 **Confidentiality. "Confidential Information"** means (a)reserved, (b) the CCO Products, (c) Feedback and (d) all CCO information and materials to which Customer has access in connection with this Agreement and all personally identifiable information including, but not limited to, name, address, date of birth, social security or other government-issued social identification numbers, income and credit histories, bank and credit card numbers, email address, and static IP address. Customer will use CCO Confidential Information solely for the Purpose and will not use, disseminate or in any way disclose any Confidential Information to any third party other than as required for the Purpose. Additionally, notwithstanding the foregoing, except as expressly permitted herein, Customer will not disclose any Confidential Information outside of the United States without CCO's prior written consent.

5.3 **Exceptions to Confidentiality.** Confidential information does not include information that (a) is or becomes part of the public domain through no act or omission of Customer or its agents or processors, (b) is rightfully obtained by Customer without breach of any obligation to maintain its confidentiality from a source other than CCO who is known or should have been known to Customer to be under no obligation to CCO or its agents or employees to maintain such information in confidence, or (c) is independently developed by Customer without using the Confidential Information. Customer may disclose Confidential Information in response to a valid court or governmental order, if (x) Customer has given CCO prior written notice and provided reasonable assistance to afford it the opportunity to object and obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information, and (y), in the opinion of Customer's counsel, Customer is compelled as a matter of law to disclose the subject Confidential Information, and (z) Customer discloses to the party compelling disclosure only the part of such Confidential Information as is required by law to be disclosed in the opinion of its counsel and uses commercially reasonable efforts to obtain confidential treatment therefor. CCO recognizes that Federal agencies are subject to the Freedom of Information Act, 5 USC. 552, which may require that certain information be released, despite being characterized

as "confidential" by the vendor.

5.4 **Breach of Confidentiality.** If there is a breach of Customer's confidentiality obligations under this Agreement, Customer will reasonably cooperate with CCO in investigating and mitigating, to the extent practicable, any damages due to such breach and/or misappropriation. Such cooperation will not relieve Customer of any liability it may have as a result of such a breach. Except to the extent required by applicable law, Customer will make no public notification, including but not limited to press releases or consumer notifications, of the potential or actual occurrence of such misappropriation and/or unauthorized disclosure without CCO's prior written consent, which consent will not be unreasonably withheld, conditioned or delayed. To the extent such public notifications are required by applicable law, Customer will provide CCO written notice prior to releasing such public notifications.

5.5 **Privacy and Data Protection.** Customer acknowledges that CCO Data may include personal information or personal data, as those terms are defined by the jurisdictions with legal authority over Customer's activities. Customer agrees to comply with all applicable privacy and data protection laws in the performance of its obligations under the Agreement, including maintaining a privacy policy that describes how it collects, uses, stores and discloses personal information, and instructs individuals how to opt-out of such practices or, if required, how to affirmatively consent to such practices, and how to contact Customer to exercise other legal rights with respect to personal information. Further, Customer agrees to provide reasonable assistance to CCO to allow CCO to fulfill its obligations under applicable privacy and data protection laws.

6 **LIMITATION OF LIABILITY.** Customer acknowledges that CCO maintains a database, updated on a periodic basis, from which Customer obtains and resells the CCO Products, and that CCO does not undertake a separate investigation for each inquiry or request for the CCO Products made by Customer. Customer also acknowledges that the prices CCO charges Customer for the CCO Products are based upon CCO's expectation that the risk of any loss or injury that may be incurred by use of the CCO Products will be borne by Customer and not CCO. Customer, therefore, agrees that it is responsible for determining that the CCO Products are in accordance with CCO's obligations under this Agreement. Customer hereby agrees to bear the risk of any liability relating to its use of the CCO Products. ACCORDINGLY, CUSTOMER'S USE OF OR ACCESS TO THE CCO PRODUCTS IS ENTIRELY AT ITS SOLE RISK. NEITHER CCO NOR ANY OF ITS DATA SUPPLIERS WILL BE LIABLE OR RESPONSIBLE TO CUSTOMER FOR ANY LOSS OF PROFITS, REVENUES, OR DATA, OR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES OR LOSSES INCURRED IN CONNECTION WITH THE CCO PRODUCTS, ANY USE OR ACCESS THEREOF OR ANY OTHER DATA OR MATERIALS TRANSMITTED THROUGH OR RESIDING ON THE NETWORK, REGARDLESS OF THE TYPE OF CLAIM OR THE NATURE OF THE CAUSE OF ACTION, EVEN IF CCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE OR LOSS. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. WITHOUT LIMITING THE FOREGOING, IN NO EVENT WILL CCO BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY BUSINESS PRACTICES OF CUSTOMER THAT VIOLATE ANY APPLICABLE LAW, STATUTE, REGULATION, CONTRACT, OR TERMS OF SERVICE AGREEMENT. CCO's liability (including the liability of any third-party data provider) and Customer's sole remedy, whether in contract, under any warranty, in tort, in strict liability or otherwise, will not exceed the return of the charges paid by Customer to CCO, subject to the maximum limit set forth in this Section. The price stated for the CCO Products is a consideration in limiting CCO's liability and Customer's remedy. IN NO EVENT WILL CCO BE LIABLE IN ANY MANNER WHATSOEVER AS A RESULT OF CCO'S OBTAINING OR FURNISHING OF THE CCO PRODUCTS. MOREOVER, CCO'S TOTAL LIABILITY UNDER THIS AGREEMENT WILL BE THE AGGREGATE AMOUNT PAID UNDER THIS AGREEMENT BY CUSTOMER FOR THE CCO PRODUCTS, WHICH ARE THE SUBJECT OF SUCH CLAIM. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

7. **RESERVED.**

8. **DISCLAIMER OF WARRANTY.** CCO will use reasonable best efforts to deliver the CCO Products to Customer; provided, however, that Customer accepts that CCO Products are provided "AS IS." Because the CCO Products involve conveying information provided to CCO by other sources, CCO cannot and will not be an insurer, guarantor or warrantor of the accuracy or reliability of the CCO Products, data contained in its database or in the CCO Products. CCO DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE CCO PRODUCTS, INFORMATION IN THE CCO PRODUCTS OR THE MEDIA ON OR THROUGH WHICH THE CCO PRODUCTS ARE PROVIDED. CCO DOES NOT GUARANTEE CONTINUOUS OR UNINTERRUPTED DISPLAY OR DISTRIBUTION OF THE CCO PRODUCTS. CCO WILL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY ANY OF CCO'S ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE CCO PRODUCTS OR INFORMATION THEREIN. CCO PROVIDES NO WARRANTIES OTHER THAN AS EXPRESSLY SET FORTH ABOVE AND DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

9. **TEMPORARY TERMINATION OF ACCESS TO NETWORK.** CCO reserves the right at any time and without prior notice to Customer to change the Network's hours of operation or to temporarily limit access to the Network in order to perform repairs, make modifications, or as a result of circumstances beyond CCO's reasonable control.

10. **TERM OF AGREEMENT.**

10.1 **Term.** This Agreement will commence on the Effective Date and will continue for a period of one (1) year (the "**Initial Term**"), after which this Agreement may be renewed for successive one (1) year terms by exercising an option, or by both parties executing a new Purchase Order in writing (the "**Renewal Term**"). The Initial Term and any Renewal Terms will be collectively referred to as the "**Term**." This subsection is subject to the early termination rights stated elsewhere in this Agreement.

10.2 **Early Termination.** When the end-user is an instrumentality of the US, recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, CCO shall reasonably proceed with the performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement.

10.3 **Effect of Expiration or Termination.** Upon the effective date of any expiration or termination of this Agreement, Customer will cease all further use and access of the CCO Products and will cause, no later than fifteen (15) days following expiration or termination of this Agreement, the destruction of all copies of and updates to the CCO Products as well as any computer files or output listings that contained any or all CCO Products. In no event will Customer retain any CCO Products. Customer will provide written certification signed by an officer of Customer that all such CCO Products have been destroyed within thirty (30) days following expiration or termination of this Agreement. The destruction procedures undertaken by Customer will be of a nature reasonable given the type of information that comprises the CCO Products and such as is reasonably necessary to prevent any misappropriation or unauthorized use of such CCO Products. All purging of CCO Products from Customer's computer systems will also be of nature reasonable given the type of information that comprises the CCO Products and such as is reasonably necessary to prevent any misappropriation or unauthorized use of such CCO Products. In no event will Customer retain any CCO Products.

10.4 **SURVIVAL.** Sections 1, 2.4-2.6, 3, 4.4, 5, 6, 7, 9, 10, 11.3, 12, 13, 14 and 15 of this Agreement, Exhibit B and any other provision that by its nature should survive will survive any expiration or termination of this Agreement. Moreover, and notwithstanding the foregoing, any expiration or termination of this Agreement will not relieve either party of any royalties, fees or other payments

due to the other party through the date of any such expiration or termination nor affect any rights, duties or obligations of either party that accrues prior to the effective date of any such expiration or termination.

11. **Representations and Warranties.** Customer represents and warrants to CCO, as of the Effective Date and such other dates as provided below, the following:
    (a) The United States Foreign Corrupt Practices Act prohibits giving money or items of value to non-United States officials to influence a non-United States government, and also prohibits giving money or items of value to any person or firm when there is reason to believe the money or item of value will be passed on to a government official in an attempt to influence a non-United States government. Customer is in compliance and will continue to comply with all requirements of the United States Foreign Corrupt Practices Act and to refrain from accepting or making payments to third parties, which would cause CCO or its data providers to violate or otherwise have liability under such Act.
    (b) Customer is an equal opportunity employer. Customer does not discriminate on the basis of race, religion, age, sex, marital status, citizenship status, sexual orientation, veteran status, medical condition, national origin, gender identity, genetic information, physical handicap or disability, or any other legally protected classification, except as may be permitted by applicable law.
    (c) As of the Effective Date, neither Customer nor any entity holding any material ownership in Customer, nor any officer or director of Customer, is the subject of any sanctions administered or enforced by the US Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), or other relevant sanctions authority (collectively, "**Sanctions**"), nor is Customer or any entity holding any material ownership in Customer, nor any officer or director of Customer, located, organized or a resident in a country or territory that is the subject of Sanctions. Customer represents and warrants that it has not, nor will it, violate any Sanctions. Customer will not in connection with this Agreement and the transactions contemplated herein fund or engage in any activities with any individual or entity or in any country or territory that, at the time of such funding or activity, is subject to Sanctions.
    (d) Customer is duly organized, existing and in good standing under the laws of the state of its incorporation. Customer has the requisite power and authority to enter into and to satisfy all of its obligations under this Agreement and any related agreements. This Agreement and the transactions contemplated hereby have been duly authorized and approved by the appropriate officers and/or other Personnel of Customer, and no further action or proceeding on the part of Customer is necessary or appropriate with respect to the execution by Customer of this Agreement or any related agreements, or the consummation by Customer of the transactions contemplated hereby or thereby.
12. **GENERAL.** This Agreement will be governed by the Federal law of the United States. This Agreement will not be assigned by Customer or CCO, in whole or in part, without the written consent of the other party. All notices to Customer that are required or permitted under this Agreement will be sent to Customer at the address listed above via certified or registered mail, return receipt requested. All notices to CCO that are required or permitted under this Agreement will be sent to CCO at the address listed above via certified or registered mail, returned receipt requested. Failure by either party to insist in any one or more cases upon the strict performance of any of the terms and conditions of this Agreement will not be considered a waiver or relinquishment for the future of any such term or condition or of any other term or condition. The terms and conditions set forth in this Agreement, together with the underlying GSA Schedule Contract, Schedule Pricelist, Purchase Order(s), constitute the entire agreement of the parties on the subject matter hereof, and any additional or different terms or conditions set forth in any other document, will be of no effect. This Agreement is not intended to create or evidence any employer-employee arrangement, agency, partnership, joint venture, or similar relationship of any kind whatsoever between CCO and Customer or any Personnel, agent or subcontractor of Customer. CCO is not responsible, and Customer is responsible for withholding, deducting or remitting from Customer Personnel's compensation, any federal or state income taxes, social security, unemployment compensation, medical, dental, workers' compensation, or disability insurance coverage, pension or retirement plans or the like. Neither party will, by virtue of this Agreement, have any right or power to create any obligation, express or implied, on behalf of any other party. Nothing herein, whether expressed or implied, is intended to confer upon any person other than the parties hereto and their respective heirs, representatives, successors and permitted assigns, any rights or remedies under or by reason of this Agreement. If any provision of this Agreement is held to be invalid, illegal or unenforceable, the provision will be enforced to the maximum extent permissible, and the validity, legality, and enforceability of the remaining provisions will continue in full force and effect to the extent the parties' intent reflected in this Agreement remains substantially unimpaired. Section headings of this Agreement are provided for reference only and will not be used as a guide to interpretation.
13. **FORCE MAJEURE.** Excusable delays shall be governed by FAR 52.212-4(f).
14. **RETENTION OF RIGHTS.** Nothing in this Agreement is intended to or will limit or restrict CCO's ability to market and sell its services within the geographic areas in which, or to the customers to whom, Customer markets or sells its services.

This is an Exhibit to, and subject to the terms of the Master Services Agreement between CCO and Customer effective as of the date set forth in the Purchase Order, Statement of Work, or similar document.

EXHIBIT A

EXHIBIT EFFECTIVE DATE:

PURPOSE (CHEC K ALL THAT APPLY):

☐ Purpose A: Internally evaluating and testing the CCO Products ("Testing")

☐ Purpose B: Performing research in the regular course of Customer's business and (b) if required, temporarily storing (on a storage device in Customer's exclusive control) and/or printing an insubstantial amount of only applicable portions of CCO Data in order to quote it in memoranda, briefs or similar work product produced in the regular course of Customer's business or to provide to Customer's clients in the regular course of Customer's business.

IF PURPOSE A (TESTING) IS CHECKED ABOVE, CHECK DURATION FOR TESTING*: days
* Note: Duration begins on the Exhibit Effective Date.

FEES:
For Purpose A (Testing), no charge during the duration.

For Purpose B, the following fees apply:

Please refer to the awarded negotiated price schedule on file for GSA Schedule 70 Contract #47QTCA19D001T, SIN categories 132-40 and 132-32.

CONFI-CHEK, INC.	**CUSTOMER:**
By:	By:
Name:	Name:
Title:	Title:

EXHIBIT B

ACCESS SECURITY REQUIREMENTS FOR INFORMATION ACCESS

Customer will maintain an information security program that is designed to protect information processing system(s) and media containing CCO Products from internal and external security threats, and CCO Products from unauthorized disclosure. Customer will be responsible to implement this program for all CCO Products to which Customer or any of its employees, consultants, agents, representatives, contractors or subcontractors ("**Personnel**") have or obtain access. CCO reserves the right to make changes to this Exhibit and its security requirements without prior notification to the Customer. The information provided in this Exhibit provides minimum baseline information security requirements. Customer agrees to follow the requirements outlined below when accessing, transmitting, processing, storing or using (collectively, "**accessing**" or "**access**") any CCO Products. Customer will strictly comply with the following:

1. **Access and Passwords.**

1.1 **CCO Products Access Control Measures**

(a) All credentials such as user names/identifiers (user IDs) and user passwords, must be kept confidential and must not be disclosed to an unauthorized party.
(b) If using a third party or proprietary system to access CCO Products, Customer will ensure that the access must be preceded by authenticating users to the application and/or system.
(c) If the third party or third-party software or proprietary system or software used to access CCO Products is replaced or no longer in use, the passwords should be changed immediately.
(d) Customer will cause a unique user ID and password to be created for each user to enable individual authentication and accountability for access to CCO's Products.
(e) User IDs and passwords will only be assigned to authorized individuals granting the least privilege necessary to perform the Personnel's responsibilities.
(f) Ensure that Personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for Permitted Purposes.
(g) Customer will ensure that no Customer Personnel access their own credit reports or those reports of any family member(s), a friend(s) or another individual unless in connection with a Permitted Purpose and applicable law.
(h) Customer will implement a process to terminate access rights immediately for users who access CCO Products when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
(i) Customer will implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.
(j) Customer will implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.2 **Use of Passwords with CCO Products.** Customer will:

(a) Require strong passwords consistent with industry best practices that: (i) cannot be easily determined (i.e., name or company name, repeating numbers and letters or consecutive numbers and letters);
(b) Ensure that passwords are not transmitted, displayed or stored in clear text
(c) Protect all end-user (e.g., internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm, also known as "one-way" encryption, when using encryption and "salting," ensure that strong encryption algorithm is utilized (e.g., AES 256 or above).
(d) Require active logins to credit information systems to be configured with an appropriate inactive session timeout.

1.3. **Change of Passwords.** Passwords (user passwords) must be changed immediately when:

(a) Any system access software is replaced by other system access software or is no longer used.
(b) The hardware on which the software resides is changed or disposed of.
(c) Any suspicion of a password being disclosed to an unauthorized party.

2. **Asset Protection.** Customer will maintain commercially reasonable controls, based on Customer's industry (or general best practices if nothing for the industry exists), in place to protect Customer's assets. This should include handling standards for introduction, transfer, removal, and disposal of all assets based on asset classification. Without limiting the foregoing, Customer will:

(a) Maintain an inventory of critical hardware and critical software assets that access, store, or make use of CCO Products.
(b) Have procedures for the disposal and reuse of equipment that access, make use of or store CCO Products, including notification procedures in the event of any lost or misplaced equipment that may have access to or store information related to CCO Products.
(c) Implement physical security controls to prevent unauthorized entry to Customer's facility and access to CCO Products. Customer will ensure that access is controlled with badge readers, other systems, or devices that restrict physical access, including but not limited to authorized lock and key.

3. **Data and Information Protection.** Customer will maintain a documented set of rules and procedures that regulate the use, access, and control of information, including without limitation its receipt, transmission, processing, storage, controls, distribution, retrieval, access, and presentation. Without limiting the foregoing, these rules will protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule. Customer will maintain a formal user registration and de-registration procedure for granting and revoking access and access rights. Without limiting the foregoing, Customer will comply with the following measure to protect all data:

(a) Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle.
(b) Implement and follow current best security practices for computer virus detection scanning services and procedures
(c) Implement and follow current best procedures for transmission, disclosure, storage, destruction, and any other information modalities or media should address all aspects of the lifecycle of the information.
(d) Encrypt all CCO Products when stored or transmitted electronically on any system using strong encryption such AES 256 or above.
(e) CCO Products are confidential and must not be stored on personally-owned equipment or portable devices, including, but not limited to, laptops, personal digital assistants, MP3 devices, USB devices, removable/portable media, or smart tablets or smartphones.
(f) When using smart tablets or smartphones to access CCO Products, ensure that such devices are protected via device passcode.
(g) Applications utilized to access CCO Products must protect data while in transmission, such as SSL protection and/or use of VPN.

(h) When no longer in use, all hard-copy materials containing CCO Products must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
(i) When no longer in use, electronic media containing CCO Products must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).
(j) Require any and all of Personnel permitted under this Agreement to have access to any CCO Products to maintain effective information security measures designed to protect CCO Products from unauthorized disclosure or use.
(k) Ensure that all data requests from Customer to CCO include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

4. **Network Protection.**
(a) Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices. Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
(b) Administrative access to firewalls and servers must be performed through a secure internal wired connection only. Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
(c) For wireless networks connected to or used for accessing or transmission of CCO Products, ensure that networks are configured and firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks.
(d) When using third-party service providers (e.g., application service providers) to access, transmit, store or process CCO Products, ensure that an independent 3rd party security assessment (one of the following, or a current equivalent: ISO 27001, PCI DSS, EI3PA, SSAE 16 – SOC 2/SOC3, FISMA, or CAI / CCM) has been performed and that they are found to be compliant.
(e) Perform regular tests/scans on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g., fix critical issues immediately, high severity in 15 days, etc.)
(f) Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit CCO Products; establish a process for linking all access to such systems and applications.
(g) Use current best practices to protect telecommunications systems, and any computer system or network device(s) used to provide CCO Products and to access CCO Products.

5. **Mobile and Cloud Technology.**
(a) Storing CCO Products on mobile, cloud, or portable devices and services is prohibited. Any exceptions must be obtained from CCO in writing; additional security requirements will apply.
(b) Mobile application development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.
(c) Mobile application development processes must follow secure software assessment methodology, which includes appropriate application security testing (for example, static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
(d) Under no circumstances are CCO Products to be exchanged between secured and non-secured applications on the mobile device.
(e) In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing CCO Products via mobile applications (internally developed or using a third-party application), ensure that multi-factor authentication mechanisms are utilized to authenticate users to the application.

6. **Personnel Background Checks, Policies, and Training.**

6.1 **Background Check.**
(a) Customer will conduct, or require, appropriate pre-employment background checks on all Personnel that have access to hardware or software systems that access, use, or store CCO Products.
(b) Customer will comply with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting pre-employment background screenings.
(c) Customer will maintain a process to enable it to learn if any Personnel are convicted of any crimes at any time after the pre-employment background screening that would have otherwise disqualified such Personnel during such pre-employment background screening. Regardless of how Customer learns of such violation, in the event such Personnel have access to CCO Products, it must promptly contact CCO to discuss the potential impact to information security and confidentiality.

6.2 **Policies and Training.**
(a) Prior to receiving access to CCO Products, Personnel will receive security awareness training appropriate to their job function.
(b) The access rights of all Personnel with access to systems or media containing CCO Products will be removed immediately upon termination of their employment, contract or agreement, or adjusted upon change of job function.
(c) Customer will require its customers to maintain effective information security measures consistent with this Agreement in order to protect confidential information from unauthorized disclosure or use of CCO Products.

7. **Security Audits.**
(a) Customer understands that its use of CCO Products and compliance with the security requirements set forth in this Exhibit may be monitored and audited by CCO. CCO may, subject to Government security requirements, from time to time conduct on-site security audits or reviews on Customer's systems containing any CCO Products as it relates to the Customer's compliance with the terms of this Exhibit or the mechanisms Customer maintains to safeguard access to CCO Products. Audits may include an examination of systems security and associated administrative practices.
(b) Reasonable access to audit trail reports of systems utilized to access CCO Products will be made available to CCO upon request, for example, during breach investigation or while performing audits.

8. **Vulnerability Monitoring; Software Development.**
(a) Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops), mobile devices, and all other systems current with appropriate system patches and updates.
(b) Configure infrastructures such as firewalls, routers, servers, tablets, smartphones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
(c) Implement and follow current best security practices for computer virus detection scanning services and procedures:
• Use, implement, and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus

technology exists.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and perform scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

9. **Security Incidents.**
   (a) Customer will have a documented plan and associated procedures in case of an information security incident. The plan must clearly articulate the responsibilities of Personnel and identify relevant notification parties.
   (b) Unless prohibited by law, Customer will notify CCO of any security breach involving (i) the theft, loss or unauthorized disclosure, acquisition, access to or misuse of the CCO Products in the possession or control of Customer; or (ii) a compromise of the confidentiality and/or integrity of any hardware, software, network, or telecommunications or information technology systems used by Customer to transmit, store, process or otherwise handle the CCO Products ("Security Breach") as soon as Customer knows or reasonably suspects that such Security Breach exists or did exist, and in any event within twenty-four (24) hours of such knowledge or suspicion. In the event Customer is prohibited by law from providing such notice, it will nonetheless provide as much of the foregoing information as it is permitted to provide under law at the earliest practicable time it is permitted to do so under law.

10. **Head Security Designate.** In addition to the above, following requirements apply where Customer or its Personnel are provided access to CCO Products directly or via the Internet ("**Internet Access**"):
   (a) Customer agrees to identify to CCO in writing an employee; it has designated to act on its behalf as a primary interface with CCO on systems access related matters. This individual will be identified as the "**Head Security Designate.**" Customer's Head Security Designate will be responsible for establishing, administering and monitoring all Customer Personnel's access to CCO Products which are delivered by Internet Access, or approving and establishing Security Designates to perform such functions
   (b) Customer will limit the dissemination of the CCO Data Products to appropriate employees whose duties justify the need to know such CCO Data Products and will require that all such employees are first subject to obligations of confidentiality substantially similar to those contained herein. Head Security Designate must immediately report any suspicious or questionable activity to CCO regarding access to CCO Products and must disable access by any employee if it is or may become likely to result in a security threat, the release or compromise of CCO Products or if the employee 's employment is terminated by Customer. CCO reserves the right to temporarily suspend any accounts it deems a security threat.

11. **Additional Security Terms.**
   (a) Customer acknowledges and agrees that Customer and each of its Personnel has an ongoing obligation to protect and ensure the confidentiality, privacy, security, and integrity of CCO Products, and the standards embodied in this Agreement are merely minimum standards of conduct in furtherance of the foregoing continuing obligation.
   (b) CCO may provide written notice to Customer of updates to CCO's information security requirements ("Updated Security Requirements"). Customer will comply with the Updated Security Requirements following a mutually agreed upon and reasonable period of time after agreeing to them in writing; provided that if the parties cannot reasonably agree to a period of time for Customer's compliance, or if Customer fails to provide CCO with a written certification of compliance within thirty (30) days after the agreed-upon compliance date, then CCO may terminate this Agreement in accordance with the Contract Disputes Act and refund Customer a pro rata portion of the unused fees already paid.
   (c) Before using any third-party service providers to access, transmit, or store CCO Products, Customer must obtain the prior written consent of CCO. Additional requirements and documentation may be required by CCO.

12. **Reserved.**

EXHIBIT C
PERMISSIBLE USES

Customer understands that CCO cannot provide legal advice regarding the appropriate uses of personal information and that it is Customer's obligation and responsibility to seek legal counsel in interpreting the applicable laws. However, regardless of the opinion of the Customer's legal counsel, CCO will allow or restrict access to CCO Products based on CCO's understanding of the applicable laws. All such decisions are the sole discretion of CCO and will be final.

GLBA PERMISSIBLE USES. The GLBA requires financial institutions and credit-reporting agencies to protect the personal financial information of customers and restricts disclosure of such information to non-affiliated third parties. CCO Products may contain information governed by GLBA. While other uses for information may be allowable under the GLBA, the purposes for which CCO will allow access to CCO Products are limited to those listed below.

- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability.
- To the extent specifically permitted or required under laws other than GLBA, and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, to self-regulatory organizations, or for an investigation on a matter related to public safety.
- To comply with federal, state, or local laws, rules, and other applicable legal requirements.
- As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer.
- Use by persons holding a legal or beneficial interest relating to the consumer.
- Use by persons acting in a fiduciary or representative capacity on behalf of, and with the implied or express consent of, the consumer.
- For required institutional risk control or for resolving consumer disputes or inquires.
  GLBA was enacted to protect the use and disclosure of non-public personal information, including, in certain instances, the use of identifying information only; and GLBA provides limited exceptions under which such information may be used; therefore, Customer hereby certifies to CCO that (a) it has determined that its use of certain identification-only products (Reference Products), including but not limited to, Credit Header Products, is pursuant to an exception under GLBA and (b) its use of the Reference Products will be for the GLBA exception(s) designated above.

Customer further acknowledges an understanding of the restrictions imposed by the FCRA. Customer agrees to only use information to locate or to further identify the subject of a search. Customer may not and will not use information, in whole or in part, to determine a consumer's eligibility for credit, for employment, or for tenant screening, nor may Customer use information for any other purpose for which Customer might properly obtain a consumer report, except in connection with the collection of a debt. If adverse action is to be taken against the subject of a search and the basis for such adverse action is information obtained or derived from information, Customer must verify such information from another source before taking such adverse action.

For a complete reading of the law, visit: http://www.ftc.gov/privacy/glbact/glbsub1.htm and https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act

CELL PHONE NUMBERS. Customer acknowledges that the government has placed restrictions upon the use of cell phone numbers. Customer agrees that any use of the cell phone numbers provided by CCO as part of the CCO Products will be used in strict accordance with all applicable laws, rules, and regulations.

DPPA PERMISSIBLE USES. The Driver's Privacy Protection Act, 18 USC. Section 2721 et seq. ("**DPPA**"), makes it unlawful for any person knowingly to obtain or disclose personal information from a motor vehicle record for any use not permitted by DPPA. CCO Products may contain information that is governed by the DPPA. Below are the uses permitted by DPPA:

- Use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out that agency's functions.
- Use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and, if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- Use in connection with any civil, criminal, administrative, or arbitral proceeding, in any federal, state, or local court agency, or before any self-regulatory body, including the service of process, investigation, and anticipation of litigation, and the execution of enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court.
- Use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating, or underwriting.
- Use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49, US Code.
- Use by any licensed private investigative agency or licensed security service for any purpose described above.

For a complete reading of the law, visit: http://www.flhsmv.gov/ddl/FedDPPAStatute.pdf

ACCESS TO AND USE OF DEATH DATA. Customer will not take any adverse action against any consumer without further investigation to verify information from the deceased data, flags, or other indicia within the CCO Products. Access to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 CFR § 1110.102(a)(1). The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("**DMF**"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 CFR § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 CFR § 1110.102(a)(1). As many credit bureau data services contain information from the DMF, Customer must be aware of and comply with its continued obligation to restrict any use of deceased flags or other indicia within the CCO Products to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with applicable FCRA or GLBA use. Customer's continued use of CCO Products affirms Customer's commitment to comply with these terms and all applicable laws.