Enformion, LLC.

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

Enformion Product Specifications

FOR PUBLIC SECTOR

Contract Number • AR3097

Contract Period • April 15, 2019, through Sept. 15, 2026

Enformion

Table of

“When it comes to quality data on a budget, it’s the best of both worlds”

- A Recent Data Customer

Contact

Contact Information

Contract Portfolio
ValuePoint (Cloud Solutions 2016-2026)

Contract Number
AR3097

Contract Period
04/15/2019 to 09/15/2026

Contractor
Enformion, LLC
1915 21st St
Sacramento, CA 95811

Website
https://www.enformion.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

Pricing
Please see individual product descriptions and associated pricing tables.

Maximum Order
$500,000

Minimum Order
$100

Geographic Coverage
Enformion provides services in all CONUS and OCONUS locations.

Point of Production
1915 21st 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.

ADA / Section 508 Compliance
Yes.

Warranty Terms
Standard

About Enformion, LLC.

Founded in 2000, Enformion, LLC is a leader in the Data-as-a-Service industry. Enformion's public and proprietary data sources provide data and intelligence to government and commercial organizations, with more than 6,000 data sources and 120 billion records.

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

Enformion partners with customers to deliver data solutions customized to their workflow. Sustaining key, long-standing strategic partnerships with a customer-centric approach, Enformion 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. Enformion'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.

Enformion 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. Enformion's consumer business is established as the well-known Internet brand, PeopleFinders.com, and continues to enjoy strong commercial success.

Enformion 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

Enformion offers the investigative web portal on the NASPO Valuepoint Cloud Solutions contract with transactional and flat-rate pricing options.

Web Application Portal

Enformion offers the investigative web portal on the NASPO Valuepoint Cloud Solutions 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 Enformion 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 theother 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 webbrowsers 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. Enformion offers our 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	Monthly Price Per Seat
001-WEB-0001	Enformion for Enterprise	$79.50
003-WEB-0001	Enformion for Civil Enforcement	$69.50

Available Add-Ons

Enformion offers search and reporting of our Core Resources to our government customers on an unlimited basis, at no additionalcost.

Core Resources are defined as those capabilities that we provide for shared access by the majority of our customers. Enformion 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

Enformion has partnered with an e pert 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 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	Price
001-WEB-0018	Social Media Search	$4.55
001-WEB-0033	On-Site Civil Service Fee	$10.37
001-WEB-0034	On-Site County Criminal Service Fee	$8.42
001-WEB-0041	Real-Time Arrest and Incarceration Search	$1.30
001-WEB-0054	Predictive Business Financial Report	$22.75
002-WEB-0002	Extra/Custom Database Connection for Agency Account (Enformion Credentialing)	$14,250.00

NASPO Pricing Schedule

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, Enformion 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.

Part Number	Product Name	Delivery	Price
001-API-2001	Find A Person	API	$0.10
001-API-2002	Reverse Phone Search	API	$0.10
001-API-2003	Business Search	API	$0.20
001-API-2004	Census Search	API	$0.10
001-API-2005	Criminal Search	API	$0.25
001-API-2006	Debt Search (Bankruptcy, Lien, Judgment)	API	$0.25
001-API-2007	Domain Search	API	$0.13
001-API-2008	Eviction Search	API	$0.13
001-API-2009	FEIN Search	API	$0.13
001-API-2010	Foreclosure Records	API	$0.13
001-API-2011	Property Search	API	$0.13
001-API-2012	Workplace Search	API	$0.13
001-API-2013	Marriage Search	API	$0.05
001-API-2014	Divorce Search	API	$0.05
001-API-2015	Professional Licenses	API	$0.25
001-API-2016	Place of Employment / Workplace	API	$0.08
001-API-2017	Enformion Identity Verification Search	API	$0.25
005-MTR-4001	Continuous Monitoring (Per Individual, Per Month)	API	$0.10
001-BAT-3001	Best Address (In Bulk)	File Drop	$0.08
001-BAT-3002	Best 3 Addresses (In Bulk)	File Drop	$0.08
001-BAT-3003	Best Phone (In Bulk)	File Drop	$0.08
001-BAT-3004	Best 3 Phones (In Bulk)	File Drop	$0.08
001-BAT-3005	Address & Phone (In Bulk)	File Drop	$0.08
001-BAT-3006	Address & Best 3 Phones (In Bulk)	File Drop	$0.08
001-BAT-3007	Criminal (In Bulk)	File Drop	$0.13
001-BAT-3008	Business (In Bulk)	File Drop	$0.15
001-BAT-3009	Bankruptcy Search (In Bulk)	File Drop	$0.10
001-BAT-3010	Liens (In Bulk)	File Drop	$0.10
001-BAT-3011	Judgements (In Bulk)	File Drop	$0.10
001-BAT-3012	Debt: BK, Liens, Judgments (In Bulk)	File Drop	$0.15
001-BAT-3013	Best Phone & Email (In Bulk)	File Drop	$0.08
001-BAT-3014	Best 3 Properties Owned by Individual (In Bulk)	File Drop	$0.15
001-BAT-3016	Deceased Records Search	File Drop	$0.15
001-BAT-3017	Household Composition Search	File Drop	$0.50

End-User Support

The data provider industry for the public sector is becoming increasingly specialized. That's why Enformion provides much more thanjust 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

Enformion 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.

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

Vendor-Provided Technical Support

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

Protecting Program Integrity

Social services programs normally accept applicant attestation of their circumstances for consideration of program eligibility. Slight inaccuracies, such as omitting an adult contributor to the household or not reporting room-rental income can incorrectly lead to an approval.

To identify these situations, social services agencies require a range of tools and resources to detect fraudulent claims applications, to identify ineligible claimants, to prioritize case investigations, and to package investigative findings for transfer to law enforcement.

The Enformion platform offers a breadth of data and investigative resources for social services program integrity:

- **Enformion Identity Verification**, delivered via API, batch, and interactively via our investigative web portal. The Enformion Identity Verification Service, implemented via API, functions as a risk-scoring mechanism for categorizing incoming applications.
- **Incarceration fraud** has always been an issue for social services agencies for a long time. Incarcerated individuals are ineligible to receive unemployment benefits as they are unable to search for employment actively. While many agencies may search their in-state records, few will search nationally.
- Enformion's **household composition** reporting outputs via batch file exchange the list of adults living in the specified household and likely relationships, such as spouses and significant others.
- Enformion's **investigative data** delivered via API, batch, and the web, is essential to identifying fraud, civil, and criminal offenses suspects while providing accurate person-locator information for contact and investigative follow-up.
- **Case selection**, inputs from Enformion API and batch file services will enable customer-side automation of classifying current, backlogged, and previously approved applicants by risk level.
- **Investigators will identify suspects** using Enformion's interactive web research portal, with access to our forty (40) years of historical records aggregation and an average of 27 known family and associates for each US adult, telephone records, utility records, criminal records, and civil records case dockets.
- Enformion's investigative content is **crossmatched** with records obtained from over 6,000 sources, hyperlinked, fully integrated, and lightning-fast. Enformion records are delivered via the web, API, and batch file exchange.
- **Multi-Factor Authentication (MFA)** using the customer's identity management for single-sign on and authentication to Enformion Web.
- **Fraud Reporting**, by matching in real-time against nationwide incarceration records, and identifying the potential for dual enrollment of social benefits in multiple states.
- **Build cases** with Enformion's web platform reference tagging and document export features. In addition to our investigative web platform, customers can retrieve Enformion's comprehensive person reports via API and batch file processing for automated processing of backlogged and previously-approved cases.
- Enformion amplifies **Pay and Chase** collections efforts. Enformion's forte is its expertise as a skip tracing platform. Our address, telephone data, household relationships, and social media locator capabilities are unique in their aggregation and are market-leading.
- **Enformion's Asset Identification** data includes real estate data nationwide by address and parcel number, with decades of previous transaction details for each, hyperlinked to the involved individuals' person records.
- **License Plate Reader** searches can verify whether a suspect's vehicle is commonly at a subject property, or not.
- **Foreclosure and Eviction notices** can provide an early-warning of families in crisis to program managers.

Enformion for Civil Enforcement (EFCE) is designed for the needs of government agencies that investigate or adjudicate claims for entitlements, benefits, welfare programs, or environmental regulations.

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

Social Services Programs

The data provided in EFCE is invaluable to those that deal with entitlement fraud and waste as it relates to social benefits, including:

- Pension and Retirement
- Tax & Revenue
- Women, Infants, and Children Vendor Adjudication (WIC)
- Health & Human Services
- Medicaid
- Unemployment Insurance

EFCE can help identify incidents of fraud and waste more quickly with instant access to premium data than traditional modes of investigation.

What's Included

- Current contact information
- Address and Phone data
- Known Relatives and Associates
- Real Property Data / Ownership
- Business Reports / Ownership
- Risk factors such as bankruptcies, liens, judgments, foreclosures, criminal records

Available Data Access

- Web platform for manual searches with seat pricing
- Customized Batch Processing for high volume demands and API access services for integration with third-party applications

Social Services Program Pricing

SKU	Product	Delivery	Commercial List	Price (NASPO Maximum)	Discount	Platform
001-API-2017	Enformion Identity Verification	API, Batch, Web	$0.50	$0.25	50%	SaaS
001-WEBI-0041	Real-Time Incarceration Search	API	$2.00	$1.30	35%	SaaS
001-BAT-3017	Enformion Household Composition	Web, Batch	$1.00	$0.50	50%	SaaS
001-API-2001	Person Search	API, Batch	$0.25	$0.10	60%	SaaS
001-BAT-3016	Deceased Records	API, Batch	$0.30	$0.15	50%	SaaS
001-API-2006	Debt Search (Bankruptcy, Lien, Judgment)	API, Batch, Web	$0.50	$0.25	50%	SaaS

*Average Social Services Program Integrity Discount: 49.17%

SkopeNow

Skopenow provides cloud-based software to automate open source intelligence investigations. Skopenow is a SaaS platform providing comprehensive digital records containing actionable insight. Skopenow reports include Social Media Data (profiles, photos, connections), Contact Data, Address Histories, and Link Analysis.

Skopenow for Enterprises

Skopenow for Enterprises provides access to Enhanced Extraction, Alerting, Business Search, Heat Mapping, Multi-Party Search, Behaviors, and the Dark Web.

Plan Details

Value Add	Skopenow accelerates the research time needed to conduct open-source intelligence (OSINT) investigations. Through proxies, users' searches are completely untraceable and anonymous, adding a layer of security.
Plan Summary	All plans noted with an 'E' will have access to Enhanced Extraction, Monitoring (12 credits per report), Keyword and Monitoring Summaries, and Facial Recognition Technology.
24-Hour Review Window	All duplicate searches conducted within 24 hours will automatically be voided. Duplicates match by name, fuzzy name, email, or phone match.

SkopeNow Pricing

SKU	Product	Delivery	Commercial List	Price (NASPO) Maximum	Discount	Platform
SKE	SkopeNow Enterprise	Web	$12,000.00	$10,800.00	10%	SaaS

*Average Discount: 10%

Sample Services Subscriber Agreement (Do Not Sign)

SAMPLE SERVICES SUBSCRIBER AGREEMENT (DO NOT SIGN)

This Master Services Agreement (together with the Exhibits attached hereto, this "**Agreement**") is entered into between Enformion, LLC ("**Enformion**"), a California corporation, having its principal place of business at 1821 Q Street, Sacramento, CA 95811, and ("**Customer**"), a , having its principal place of business at . The Master Services Agreement, together with Exhibits B and C is effective as of ("Effective Date") and each Exhibit A is effective as of the effective data stated on that Exhibit A. Enformion 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:
"Enformion API" means an application programming interface provided by Enformion to Customer that allows Customer to submit Search Requests to the Enformion API.
"Enformion Data" means data that is obtained from the Enformion Services or Network, all of which is comprised of publicly available information as that term is defined by the regulations prescribed under the GLBA, and that includes all languages, editions, issues, versions, revisions, modifications, enhancements and updates thereto during the Term of this Agreement.
"Enformion Products" means Enformion Services, Network, Enformion API and/or Enformion Data, together with any Enformion Confidential Information.
"Enformion Services" means the nationwide public record information, document retrieval and related services provided by Enformion through the Network.
"FCRA" means the Fair Credit Reporting Act, 15 U.S.C.A. § 1681, et seq., as now or hereafter amended.
"GLBA" means the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., as now or hereafter amended.
"Network" means Enformion's online data retrieval system of proprietary databases and data and information obtained from third parties.
"Permitted Uses" means the use of Enformion Products in a manner strictly in accordance with purposes permitted under this Agreement and in compliance with all applicable laws and regulations, including, but not limited to, the GLBA and the FCRA.
"Search Request" means a search for Enformion Data through the Enformion API by Customer.

2. SERVICES AND LICENSE.

2.1. Products; Purpose. Enformion provides Enformion Products. Customer hereby agrees to use the Enformion Products for the sole purpose as set forth in Exhibit A (the "Purpose").

2.2. License. Enformion hereby grants to Customer a nonexclusive, nonassignable, nontransferable, limited license to use the Enformion Products solely for the Purpose. Nothing in this Agreement is intended to, or should be construed to prevent Enformion from entering into similar agreements with other persons or entities regarding all or any part of the Enformion 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 Enformion Products to build its own database or accumulate any Enformion Products or content for any other use; or (ii) copy or reproduce any portion of the Enformion Products; or (iii) redistribute, disclose, market, rent, lease, solicit, supply or transfer to any third party any portion of the Enformion Products; or (iv) store any results returned by the Enformion 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 Enformion Data, or is based on or having its origin in Enformion Data.

(b) Customer will not disassemble, decompile, or in any way reverse engineer the Enformion Products.

(c) Customer will comply with the then current Enformion policies and procedures as communicated by Enformion from time to time ("**Policies**"). Enformion may, from time to time, notify Customer of additional, updated or new Policies. Customer's compliance with such Policies will be a condition of Enformion's continued provision of the Enformion Products hereunder.

(d) Customer will only use the Enformion Products for the Purpose.

(e) Customer will not market the Enformion Products under the Enformion name.

(f) Customer will not distribute, provide, license, transfer or sell the Enformion Products to any third parties.

(g) Upon receipt of any updated Enformion Products from Enformion, Customer will promptly replace and destroy any outdated Enformion Products in its possession prior to the update.

(h) Customer will not merge any Enformion 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 Enformion Products or in any way compile and/or offer for use or sale any Enformion 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, Enformion may, for any reason whatsoever, suppress or remove information pertaining to one or more particular persons from the Enformion Data ("**Removals**"). Enformion 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 Enformion, Customer will: (a) remove or suppress such persons who are the subject of the Removals from any and all materials provided by Enformion to Customer; and (b) exclude such persons who are the subject of the Removals from any Enformion 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 Enformion Products as reasonably requested by Enformion. Feedback becomes the exclusive property of Enformion and is Enformion Confidential Information.

3. COMPLIANCE WITH LAWS; SECURITY OF DATA.

3.1. Compliance with Laws. Customer will not use the Enformion 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 Enformion 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 Enformion Products will not be merged with consumer reports as such term is defined in the FCRA. Enformion reserves the right to insert certain information (sometime referred to as seeding) into the data available from the Enformion Products for the purpose of determining Customer's compliance with the terms of this Agreement. Misuse of the Enformion Products will constitute a material breach of this Agreement.

3.2. Privacy and Security Requirements. Customer will comply with all applicable laws concerning the Enformion 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 protect the Enformion Products in a secure manner, including without limitation, maintaining an information security program that is designed to protect information processing system(s) and media containing the Enformion Products from internal and external security threats, and the Enformion 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. Enformion 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 Enformion 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 Enformion the applicable charges as set forth in Exhibit A of this Agreement. Any periodic and/or minimum Customer fees under this Agreement are non-refundable, in whole or in part, in the event of a termination of this Agreement, since all such fees are compensation for supplying service and carrying the account. Enformion reserves the right to change the fees by issuing a revised rate schedule, but no change in such charges will become effective as to Customer earlier than thirty (30) days after written notice thereof will have been given by Enformion to Customer. Customer will also pay all the cost of all media, media shipping and insurance costs, taxes, duties or charges of any kind imposed by any federal, state, or local governmental entity for the Enformion Products provided under this Agreement. However, Customer will not be responsible for taxes imposed upon Enformion by any federal, state or local authority against the net income of Enformion. Payment inquiries should be remitted in writing to the following address: Enformion, 1915 21st Street, Sacramento, CA 95811, or by fax to (916) 739-1118.

4.2. Invoicing and Payment. Unless otherwise expressly stated in Exhibit A to this Agreement, Customer will pay all invoices from Enformion issued pursuant to this Agreement within thirty (30) days of the invoice date.

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

(a) amounts which are not paid within sixty (60) days of the invoice date or the date on which Enformion notifies Customer, whichever is sooner, may be subject to a late charge of one and one-half percent (1.5%) per month (18% per year) or the maximum allowed by law, whichever is less. If collection efforts are required, Customer will pay all costs of collection, including reasonable attorneys' fees.

(b) Enformion reserves the right to immediately suspend Customer's access to Enformion Products until any unpaid or past due amounts are paid in full.

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, Enformion will have access to those records of Customer that are necessary to determine Customer's compliance with its obligations under this Agreement and to Customer's facilities for the purpose audit either through its own employees, representatives or an independent public accounting firm selected by Enformion (the "**Auditor**"). Any such review of Customer's records, facilities, or both, may be conducted during Customer's normal business hours upon Enformion 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 Enformion Product-related services to Customer, from time to time, Enformion will have the right to review, at Enformion's expense, each such third party's security processes and procedures related to the transmission, storage or processing of Enformion Products. Customer will reasonably cooperate, and will request each such third party to also reasonably cooperate, with Enformion and any Enformion requests in conjunction with all such reviews including, but not limited to Enformion requests to correct any deficiencies discovered during such audits within a period of time mutually agreed upon and/or suspend any further transmission of Enformion Products until such deficiencies are corrected. Customer agrees that it will reasonably cooperate with all such reasonable Enformion 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 Enformion.

5. INTELLECTUAL PROPERTY; CONFIDENTIALITY.

5.1. Intellectual Property. Customer acknowledges that Enformion has expended substantial time, effort, and funds to collect, arrange, compile create and deliver the Enformion Products. Customer agrees not to reproduce, retransmit, republish, or otherwise transfer for any commercial or other purpose any information that Customer receives from Enformion or the Enformion Products except as permitted under this Agreement. Customer acknowledges that Enformion (and/or Enformion's third-party data providers) will retain all right, title, and interest in and to the data and information provided by the Enformion Products and to Derivative Matter under applicable contractual, copyright, intellectual property and related laws, and Customer will use such materials consistent with Enformion's interests and notify Enformion of any threatened or actual infringement of Enformion's rights. Customer further acknowledges and agrees that it will acquire no right, title or interest under applicable copyright or other laws in the Enformion 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 Enformion Products. "**Derivative Matter**" means any work, invention, new material or data which is based in whole or in part upon the Enformion Products and any intellectual property rights associated therewith, including without limitation derivative work, improvement, extension, revision, modification, translation, compilation, or error correction.

5.2. Confidentiality. "**Confidential Information**" means (a) the terms and conditions of this Agreement, (b) the Enformion Products, (c) Feedback and (d) all Enformion information and materials to which Customer has access in connection with this Agreement and all non-public personally identifiable information including, but not limited to, name, address, date of birth, social security or other government issued social identification number, income and credit histories, bank and credit card numbers, email address, and static IP address. Customer will use Enformion 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, Enformion may disclose the terms and conditions of this Agreement to Enformion's agent(s) and/or processor(s) under appropriate nondisclosure terms solely to the extent necessary to fulfill its obligations under this Agreement. Except as expressly permitted herein, Customer will not disclose any Confidential Information outside of the United States without Enformion'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 Enformion who is known or should have been known to Customer to be under no obligation to Enformion 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 Enformion 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.

5.4. Breach of Confidentiality. If there is a breach of Customer's confidentiality obligations under this Agreement, Customer will reasonably cooperate with Enformion 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 Enformion'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 Enformion written notice prior to releasing such public notifications.

7.1. No Suit. Customer covenants not to sue or maintain any cause of action, claim, demand, cross-claim, third party action or other form of litigation or arbitration against Enformion, its officers, directors, employees, contractors, agents, affiliated bureaus or Customers arising out of or relating in any way to the Enformion Products not being accurate, timely, complete or current.

8. DISCLAIMER OF WARRANTY. Enformion will use reasonable best efforts to deliver the Enformion Products to Customer; provided, however, that Customer accepts that Enformion Products are provided "AS IS." Because the Enformion Products involve conveying information provided to Enformion by other sources, Enformion cannot and will not be an insurer, guarantor or warrantor of the accuracy or reliability of the Enformion Products, data contained in its database or in the Enformion Products. ENFORMION DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE ENFORMION PRODUCTS, INFORMATION IN THE ENFORMION PRODUCTS OR THE MEDIA ON OR THROUGH WHICH THE ENFORMION PRODUCTS ARE PROVIDED. ENFORMION DOES NOT GUARANTEE CONTINUOUS OR UNINTERRUPTED DISPLAY OR DISTRIBUTION OF THE ENFORMION PRODUCTS. ENFORMION WILL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY ANY OF ENFORMION'S ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE ENFORMION PRODUCTS OR INFORMATION THEREIN. ENFORMION 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. Enformion reserves the right at any time and without prior notice to Customer to change the Network's hours of operation or to limit access to the Network in order to perform repairs, make modifications or as a result of circumstances beyond Enformion's reasonable control.

10. **Representations and Warranties.** Customer represents and warrants to Enformion, 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 Enformion 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 U.S. 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 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.
11. **FORCE MAJEURE.** Neither party will be liable to the other for failure to perform or delay in performance under this Agreement if, and to the extent, such failure or delay is caused by conditions beyond its reasonable control and which, by the exercise of reasonable diligence, the delayed party is unable to prevent or provide against. Such conditions include acts of God; strikes, boycotts or other concerted acts of workmen; failure of the Internet, utilities or networks; laws, regulations or other orders of public authorities; military action, state of war or other national emergency; fire or flood.
12. **RETENTION OF RIGHTS**. Nothing in this Agreement is intended to or will limit or restrict Enformion'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.

ENFORMION, LLC	**CUSTOMER:**
By:	By:
Name:	Name:
Title:	Title:

End-User License

This is an Exhibit to, and subject to the terms of the Master Services Agreement between Enformion and Customer effective .

EXHIBIT A- (insert number; change for additional Exhibit As)

EXHIBIT EFFECTIVE DATE:

PURPOSE (CHECK ALL THAT APPLY):

☐ Purpose A: Internally evaluating and testing the Enformion 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 Enformion 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 duration.

For Purpose B, the following fees apply:

INVOICING AND PAYMENT (INSERT ONLY IF DIFFERENT FROM SECTION 4.2 OF THE AGREEMENT):

ENFORMION, LLC	**CUSTOMER**:
By:	
Name:	
Title:	

SAMPLE – DO NOT SIGN

EXHIBIT B

ACCESS SECURITY REQUIREMENTS FOR NON-PUBLIC INFORMATION ACCESS

Customer will maintain an information security program that is designed to protect information processing system(s) and media containing Enformion Products from internal and external security threats, and Enformion Products from unauthorized disclosure. Customer will be responsible to implement this program for all Enformion Products to which Customer or any of its employees, consultants, agents, representatives, contractors or subcontractors ("**Personnel**") have or obtain access. Enformion reserves the right to make changes to this Exhibit and its security requirements without prior notification to 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 Enformion Products. Customer will strictly comply with the following:

1. Access and Passwords.

1.1. **Enformion 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 third party or proprietary system to access Enformion 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 Enformion 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 Enformion'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), friend(s) or other 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 Enformion 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 Enformion 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 are 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.
(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 Enformion Products.
b) Have procedures for the disposal and reuse of equipment that access, make use of or store Enformion Products, including notification procedures in the event of any lost or misplaced equipment that may have access to or store information related to Enformion Products.
c) Implement physical security controls to prevent unauthorized entry to Customer's facility and access to Enformion 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 Enformion Products when stored or transmitted electronically on any system using strong encryption such AES 256 or above.
e) Enformion 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 smart phones.
f) When using smart tablets or smart phones to access Enformion Products, ensure that such devices are protected via device pass-code.
g) Applications utilized to access Enformion 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 Enformion 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 Enformion 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 Enformion Products to maintain effective information security measures designed to protect Enformion Products from unauthorized disclosure or use.
k) Ensure that all data requests from Customer to Enformion 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 Enformion 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 Enformion 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 Enformion 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 Enformion Products and to access Enformion Products.

5. Mobile and Cloud Technology.

a) Storing Enformion Products on mobile, cloud or portable devices and services is prohibited. Any exceptions must be obtained from Enformion in writing; additional security requirements will apply.

b) Mobile applications 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 applications 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 Enformion 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 Enformion Products via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication mechanisms are utilized to authenticate users to 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 Enformion 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 Enformion Products, it must promptly contact Enformion to discuss the potential impact to information security and confidentiality.

(d) All Personnel must be bound by Non-Disclosure/Confidentiality Agreement before they perform any service requiring access to Enformion Products.

6.2. Policies and Training.

(a) Prior to receiving access to Enformion 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 Enformion 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 Enformion Products.

7. Security Audits.

a) Customer understands that its use of Enformion Products and compliance with the security requirements set forth in this Exhibit may be monitored and audited by Enformion. Enformion may from time to time conduct on-site security audits or reviews on Customer's systems containing any Enformion Products as it relates to the Customer's compliance with the terms of this Exhibit or the mechanisms Customer maintains to safeguard access to Enformion Products. Audits may include examination of systems security and associated administrative practices.

b) Reasonable access to audit trail reports of systems utilized to access Enformion Products will be made available to Enformion 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 infrastructure such as firewalls, routers, servers, tablets, smart phones, 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 performs 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 Enformion of any security breach involving (i) the theft, loss or unauthorized disclosure, acquisition, access to or misuse of the Enformion Products in the possession or control of Customer or any Authorized End User; or (ii) a compromise of the confidentiality and/or integrity of any hardware, software, network, or telecommunications or information technology systems used by Customer or its Authorized End Users to transmit, store, process or otherwise handle the Enformion 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. Email notification at support@enformion.com.

10. Head Security Designate. In addition to the above, following requirements apply where Customer or its Personnel are provided access to Enformion Products directly or via Internet **("Internet Access")**:

a) Customer agrees to identify to Enformion in writing an employee it has designated to act on its behalf as a primary interface with Enformion 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 Enformion 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 Enformion Data Products to appropriate employees whose duties justify the need to know such Enformion 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 Enformion regarding access to Enformion 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 Enformion Products or if the employee 's employment is terminated by Customer. Enformion reserves the right to terminate 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 Enformion Products, and the standards embodied in this Agreement are merely minimum standards of conduct in furtherance of the foregoing continuing obligation.

(b) Enformion may provide written notice to Customer of updates to Enformion'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; provided that if the parties cannot reasonably agree to a period of time for Customer's compliance, or if Customer fails to provide Enformion with a written certification of compliance within thirty (30) days after the agreed upon compliance date, then Enformion may terminate this Agreement without any penalty or further obligation.

(c) Before using any third party service providers to access, transmit, or store Enformion Products, Customer must obtain the prior written consent of Enformion. Additional requirements and documentation may be required by Enformion.

12. Breach. Without limiting Enformion's rights or Customer's obligations under any other provision of this Agreement, in the event of a breach by Customer of this Agreement that results in the theft, loss, or unauthorized disclosure, acquisition, access to or misuse of Enformion Products, direct damages in connection with any such breach will include (i) the reasonable costs and expenses of investigation and analysis (including by law firms and forensic firms retained by Enformion, to the extent Customer does not share its investigation and analysis work product, or such work product is not reasonably acceptable to Enformion), (ii) reasonable costs of correction or restoration of any destroyed, lost or altered data or assets, notification to affected consumers (including by mail house firms), and (iii) costs of credit monitoring and other reasonably required remediation services. Customer will reimburse Enformion for any losses incurred by Enformion in correcting Customer's failure to comply with the privacy and/or confidentiality provisions of this Agreement, including Customer's destruction obligations.

EXHIBIT C
PERMISSIBLE USES

Customer understands that Enformion cannot provide legal advice regarding the appropriate uses of non-public, 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 Customer's legal counsel, Enformion will allow or restrict access to Enformion Products based on Enformion's understanding of the applicable laws. All such decisions are the sole discretion of Enformion and will be final.

GLBA PERMISSIBLE USES. The GLBA requires financial institutions and credit-reporting agencies to protect personal financial information of customers, and restricts disclosure of such information to non-affiliated third parties. Enformion Products may contain information governed by GLBA. While other uses for non-public records may be allowable under the GLBA, the purposes for which Enformion will allow access to Enformion 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 Enformion 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 non-public information to locate or to further identify the subject of a search. Customer may not and will not use non-public information, in whole or in part, to determine a consumer's eligibility for credit, for employment, or for tenant screening, nor may Customer use non-public information for any other purpose for which Customer might properly obtain a consumer report, except in connection with 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 non-public 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 Enformion as part of the Enformion Products will be used in strict accordance with all applicable laws, rules and regulations.

DPPA PERMISSIBLE USES. The Driver's Privacy Protection Act, 18 U.S.C. 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. Enformion 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, U.S. Code.
- Use by any licensed private investigative agency or licensed security service for any purpose described above.

For a more 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 Enformion 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 C.F.R. § 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 C.F.R. § 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 C.F.R. § 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 Enformion 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 Enformion Products affirms Customer's commitment to comply with these terms and all applicable laws.

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the followingdocuments:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. TheNASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enterinto a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of

the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventingany unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “HighRisk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorizationof Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shallturn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release ofany information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations;and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Propertyrights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor

and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance describedin this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage,

with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shallhave been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the

authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies

and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of thePurchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during theterm of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this MasterAgreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnishedsolely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separateindefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or

amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific languagein some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorizedby individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate inthrough execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this MasterAgreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign theirown Participating Addendum, subject to the approval of participation by the Chief

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the MasterAgreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. Thisfee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system)specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractorshall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity'sData during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any otherterm or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as “new.”

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity’s or Purchasing Entity’s State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall bein the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity’s State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered intoa multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time theOrder is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities,other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experienceszero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiationswith and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePointprocurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed importantto the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well asContractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor toterminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

[Intentionally Left Blank]