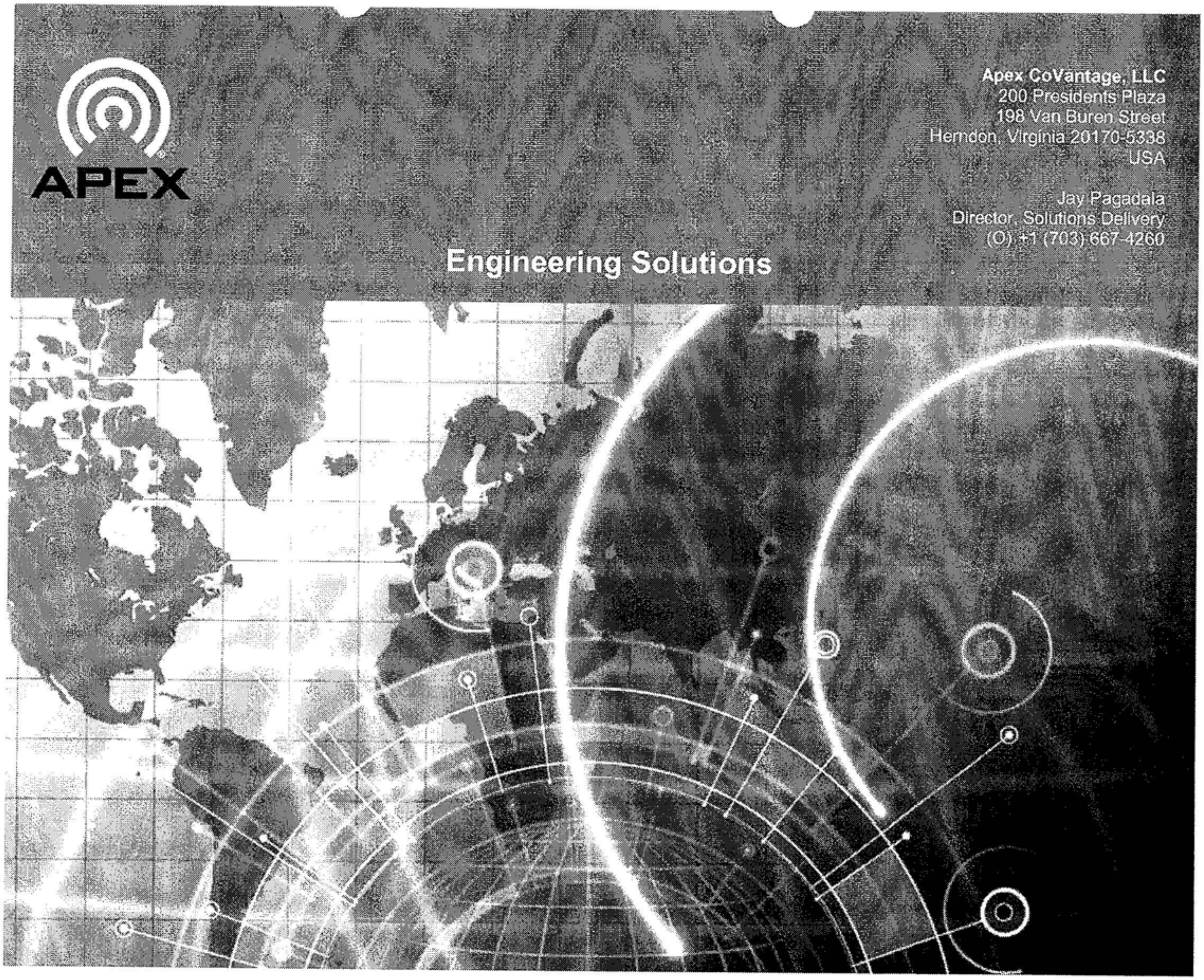


APEX

Apex CoVantage, LLC
200 Presidents Plaza
198 Van Buren Street
Herndon, Virginia 20170-5338
USA

Jay Pagadala
Director, Solutions Delivery
(O) +1 (703) 667-4260

Engineering Solutions

State of Nebraska
RFP No. 3008Z1
Broadband Data Collection and Mapping Services
Technical Proposal

September 13, 2009

Contents

List of Figures

List of Tables

ProACT®, IZAAC® and ProField™ are registered Marks or Marks of Apex CoVantage, LLC in the United States and other countries. Other product and company names mentioned herein might be registered Marks or Marks of their respective owners

The terms and conditions of this proposal are valid for ninety (90) days from the date of this proposal unless otherwise extended in writing by Apex

1.0 State of Nebraska Request for Proposal for Contractual Services

On the following page, please find the required form.

State of Nebraska (State Purchasing Bureau)

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

RETURN TO:
State Purchasing Bureau
301 Centennial Mall South, 1st Fl
Lincoln, Nebraska 68508
OR
P.O. Box 94847
Lincoln, Nebraska 68509-4847
Phone: 402-471-2401
Fax: 402-471-2089

SOLICITATION NUMBER	RELEASE DATE
RFP 3008Z1	**August 13, 2009**
OPENING DATE AND TIME	PROCUREMENT CONTACT
September 14, 2009, 2:00 p.m. Central Time	**Todd Dlouhy**

This form is part of the specification package and must be signed and returned, along with proposal documents, by the opening date and time specified.

PLEASE READ CAREFULLY!

SCOPE OF SERVICE

The State of Nebraska, Administrative Services (AS), Materiel Division, Purchasing Bureau, is issuing this Request for Proposal, RFP Number 3008Z1 for the purpose of selecting a qualified contractor to provide Broadband Data Collection and Mapping Services.

Written questions are due no later than August 21, 2009, and should be submitted via e-mail to matpurch.dasmat@nebraska.gov. Written questions may also be sent by facsimile to (402) 471-2089.

Bidder should submit one (1) original, ten (10) copies of the entire proposal. In the event of any inconsistencies among the proposals, the language contained in the original proposal shall govern. Proposals must be submitted by the proposal due date and time.

PROPOSALS MUST MEET THE REQUIREMENTS OUTLINED IN THIS REQUEST FOR PROPOSAL TO BE CONSIDERED VALID. PROPOSALS WILL BE REJECTED IF NOT IN COMPLIANCE WITH THESE REQUIREMENTS.

1. Sealed proposals must be received in State Purchasing by the date and time of proposal opening indicated above. No late proposals will be accepted. No electronic, e-mail, fax, voice, or telephone proposals will be accepted.
2. This form "REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES" MUST be manually signed, in ink, and returned by the proposal opening date and time along with bidder's proposal and any other requirements as specified in the Request for Proposal in order to be considered for an award.
3. It is the responsibility of the bidder to check the website for all information relevant to this solicitation to include addenda and/or amendments issued prior to the opening date. Website address is as follows: http://www.das.state.ne.us/materiel/purchasing/
4. It is understood by the parties that in the State of Nebraska's opinion, any limitation on the contractor's liability is unconstitutional under the Nebraska State Constitution, Article XIII, Section 3, and that any limitation of liability shall not be binding on the State of Nebraska despite inclusion of such language in documents supplied with the contractor's bid or in the final contract

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Request For Proposal For Contractual Services form, the bidder guarantees compliance with the provisions stated in this Request for Proposal, agrees to the terms and conditions (see Section III) and certifies bidder maintains a drug free work place environment.

FIRM: Apex CoVantage, LLC

COMPLETE ADDRESS: 198 Van Buren Street, Ste. 200, Herndon VA 20170

TELEPHONE NUMBER: +1 (703) 709-3000 FAX NUMBER: +1 (703) 709-8242

SIGNATURE: ______ DATE: September 11, 2009

TYPED NAME & TITLE OF SIGNER: Srini Vasan, Chief Commercial Officer

2.0 Executive Summary

Apex CoVantage, LLC is pleased to submit this proposal to the State of Nebraska for its State Broadband Data Development program to provide broadband mapping data collection and field verification services.

Apex is a privately held, certified minority-owned U.S. corporation founded in 1988, possessing extensive experience in Telco field asset studies, GIS mapping, and Telecom field surveys. Apex provides a full range of GIS mapping and engineering solutions to the telecom and utility industries through a network of associate delivery centers with a collective capacity of over 1000 engineers working on a real-time basis. Apex is a true technology services company that applies leading industry practices to drive high quality and high-value results. We balance effective project management, leading technical systems, and exceptional industry expertise to deliver responsive and reliable solutions to our customers. Our professional staff includes engineers and technicians who are leaders in this field, and can deliver exceptional service to the State of Nebraska.

The National Telecommunications and Information Administration's (NTIA) NOFA for the State Broadband Data and Development Grant Program requires substantial effort across a variety of work streams in a short timeframe. Apex has therefore adopted an approach combining best-of-class capabilities for the various aspects of the work. At the helm, to orchestrate a successful and effective program, needs to be a company that not only has a very broad and deep understanding of the work itself, but also possesses experience in managing large projects and the technology platform to effectively deploy large field crews.

Apex is responding to this RFP as the prime contractor, partnering with CSU, Chico Research Foundation (CSU Foundation). CSU Foundation, experienced in providing Broadband Mapping services in the State of California, is the not-for-profit extension for the California State University and will be providing subject matter expertise and consulting services to this project. CSU Foundation possesses extensive experience working with the California Public Utilities Commission (CPUC) and the California Emerging Technology Fund (CETF) and providing broadband demand and supply aggregation as well as broadband mapping services.

CSU Foundation has been engaged in mapping Broadband coverage areas for the California Public Utility Commission (CPUC) for the past year and a half. CSU Foundation also is thoroughly familiar with the Federal Broadband Mapping requirements through its support to over 200 Internet Service Providers making application for Broadband infrastructure subsidies under the American Recovery and Reinvestment Act of 2009. CSU Foundation provided coverage mapping services and data research services to California Internet Service Providers making BTOP and RUS funding applications.

Apex, along with CSU Foundation, commits to ensuring that local entities are engaged so that most of the employment is provided to residents of the State of Nebraska in order to further the basic goal of the American Recovery and Reinvestment Act (ARRA) to stimulate the economy.

As a part of its work efforts over the past 18 months in support of a variety of initiatives in the State of California, CSU has facilitated a public/private partnership with all the appropriate

Stakeholders in an effort to provide a collaborative approach to Broadband development. Through over 26 county meetings attended by county and municipal elected and administrative leaders, Internet Service providers (both wireline and wireless), key anchor institutions (K-12 schools, libraries, medical and healthcare institutions, public safety officials, community colleges, and universities (both public and private).

Apex is confident that with the technical resources and staff available at its disposal, combining these with CSU's experience, can facilitate the acquisition of data needed to successfully support this effort. Further, the Apex-CSU team knows of no other process or organization that has been able to successfully deliver similar coverage maps to the degree of accuracy that CSU Foundation has been able to do so within California. Further, the CSU Foundation has done this in a manner that is non-controversial, non-confrontational, and supportive of the state's objectives.

In addition to the core requirement of developing a field-verified broadband map, Apex believes that higher value and benefits can be derived by a mapping service provider who has a good mix of technology, experience, research orientation, scale of operations, and social outlook. For effective implementation of these key points, the team of Apex CoVantage and CSU Foundation is uniquely qualified to work with State of Nebraska's Broadband Data Development program, as illustrated and substantiated throughout this proposal.

2.1 Summary of Services Provided

2.1.1 Service Provider Interaction

Apex will develop a comprehensive list of facilities-based broadband providers from the list of State Filers made available through FCC Public Notice DA 09-1695 and will work with them to build a relationship, including discussing the data mapping project, the collective benefits of the project, and a request for participation. These discussions will be aimed at creating a better understanding with each provider about the operations of each network, how data is stored, which data are relevant to the project goals, the most effective method(s) for sharing and updating data for the next five years, and how non-disclosure agreements should be structured to ensure confidential information is protected while data are effectively translated to accurately represent broadband availability.

2.1.2 Working with Smaller Service Providers

Apex wishes to make their engineering staff available to smaller broadband providers to assist in the data collection/transfer/verification process. Apex will assist providers where relevant data is not stored or readily available. Apex will ensure this process is completed in a confidential manner. Such data submitted to Apex by the providers will be normalized, cleansed, and converted into a usable GIS format.

2.1.3 Updating Availability Data

Apex will translate provider data into a preliminary representation of broadband availability for each provider's service area. Apex will work directly with providers through a confidential iterative process whereby the preliminary maps are refined until both Apex and the provider believe the maps are accurate. Apex will be responsible for data gathering and relationship building with providers, and for transition and analysis of the data. This process will include constructing engineering and wireless propagation studies, developing GIS datasets, and analyzing data to develop the corresponding demographic map components.

Apex will process provider datasets as received by November 1, 2009. To the extent possible, provider data will be continued to be solicited, gathered, and processed after this date for inclusion in a final mapping data deliverable. The final mapping data deliverable will attempt to represent at least 95% of the broadband coverage within the state.

2.1.4 Online Data Collection, Speed Tests, and End User Engagement

Apex will develop and launch a website, specifically for Nebraska and equip the site with an upstream/downstream speed test tool to measure broadband upload and download speeds at the county level of detail. The site will be available to consumers across the state to test their actual upstream and downstream transmission speeds.

Apex will develop a targeted media campaign to build awareness of consumer's ability to test their broadband speed through the online website that Apex will build for the state consumer speed test site. Following the launch, Apex and the State of Nebraska will jointly determine whether there are other reasonable outreach measures that can be taken to increase the number of speed tests, either statewide or within certain counties, if numbers are lower than necessary for statistically relevant reporting.

2.1.5 Substantial Data Delivery

On or before February 1, 2009, Apex will provide a substantially complete set of data to the State. If requested by the State, Apex will provide sample maps in varying media.

Apex agrees to permit third-party entity(s) to perform verification audit of any and all data at any location. Apex is willing to share and collaborate with the Auditor all information required to determine data validity.

2.1.6 Final Deliverable

Apex will develop a full-feature State website that will have an easy-to-understand interface to allow users to drill down from the State level, through the various geopolitical and census boundaries, down to individual street segments. The map will be searchable by street segment and, to the extent possible, provide the type of technology, speed tiers, and number of providers available. Users will be able to generate pre-defined reports, construct different views based on service availability, types, and speeds, and perform a variety of on-the-fly queries using the underlying database. Apex will monitor the use patterns regularly and create additional pre-defined reports based on the most frequently performed searches and queries.

Apex will also provide the shape files associated with the broadband mapping that are ArcGIS compatible, delineate between where broadband is provided and is not, and are an aggregation of all providers participating in the State of Nebraska's mapping initiative.

Apex will work to develop, and make available, the market data analysis and maps that can be generated using existing datasets Apex has purchased or those that are made publicly available. These deliverables include county level maps showing the density of households in areas lacking broadband availability.

2.1.7 Ongoing Support and Maintenance

Apex will include information on how the public and service providers can provide feedback, report inaccuracies, and ask questions about the maps directly on the website. Resources will include, but not be limited to, a direct online form, a toll-free telephone number, and an e-mail communications options. In consultation with service providers, Apex will investigate inaccuracies reported and adjust the maps as appropriate.

Apex will continue to maintain the maps and an online interactive (searchable) version of the maps for initial period of two years or longer, as may be mutually agreed upon with the State, or until such time as the State may engage another broadband mapping provider for purposes substantially similar to those outlined in the Contract.

2.1.8 Progress Monitoring

Apex will submit quarterly reports to the State that will include efforts contributed to the project, project progress reports, funds availability versus spending, and other information as required. Apex will submit a final project status report to the State upon completion of the project.

3.0 Corporate Overview

3.1 Bidder Identification and Information

Apex CoVantage LLC is a privately held, employee-owned company, founded in 1988. Apex's **Engineering Solutions** provides a full range of GIS mapping and engineering solutions to the telecom and utility industries. Our professional staff includes engineers and technicians who are leaders in this field, and can deliver exceptional service to the State. Apex's **Technology Products and Solutions** group focuses on our mission of delivering knowledge services by leveraging the latest telecommunications and software technologies. The TPS group has developed processes and software to improve production and project management, technology, quality, and knowledge services for a wide variety of industries.

Apex is a certified, minority-owned U.S. Limited Liability Corporation; see Appendix C for copies of Apex's minority certifications. Apex is privately held by employees, with the majority share held by its founders, Dr. Shashikant Gupta and Ms. Margaret Boryczka. Dr. Gupta, CEO, and Ms. Boryczka, COO, are both actively involved in the day-to-day operations and management of the company.

Apex was incepted in 1988 as Apex Data Services, Inc. In February 2003, Apex CoVantage, LLC was formed as a wholly owned subsidiary. Our FEIN is 02-0673681.

<u>Apex Contact Information</u>

Apex CoVantage, LLC
198 Van Buren Street
Suite 200
Herndon, VA 20170
Phone: +1 (703) 709-3000
Fax: +1 (703) 709-8242
www.apexcovantage.com

3.2 Financial Statements

As a privately-held company, Apex has a policy of strictly maintaining the confidentiality of financials. One copy of our 2008 financial statement has been included in a sealed envelope; Apex respectfully requests that you maintain the confidentiality of this information.

As required, below please find Apex's banking reference:

Chevy Chase Bank, a division of Capital One, N.A.
Richard L. Amador
Senior Vice President
7926 Jones Branch Drive, Suite 230
McLean, VA 22102
Phone: 703-287-7233
Fax: 703-287-7244
Email: RLAmador@chevychasebank.net

There are no judgments, pending or expected litigation, or other financial reversals that might affect Apex.

3.3 Change of Ownership

No change in ownership or control of the company is anticipated in the future.

3.4 Office Location

Apex's corporate office location is identified in Section 3.1. Should Apex be awarded the contract, we would open an office in the state of Nebraska to better facilitate project activities.

3.5 Relationships with the State

Neither Apex nor CSU Foundation has contracted with the State previously.

3.6 Bidder's Employee Relations to State

No party within Apex's proposal response is or was an employee of Nebraska within the past twelve months. No employee of any agency of the State of Nebraska is employed by Apex or is a subcontractor.

3.7 Contract Performance

Neither Apex nor CSU Foundation has had a contract terminated for default. Neither Apex nor CSU Foundation has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason within the past three years.

3.8 Summary of Bidder's Corporate Experience

Apex possesses extensive experience in Telco field asset studies, GIS mapping, and Telecom field surveys. Apex is a true technology services company that applies leading industry practices to drive high quality and high-value results. We balance effective project management, leading technical systems, and exceptional industry expertise to deliver responsive and reliable solutions to our customers.

Apex has over 20 years of experience in providing GIS mapping, Telecom landbase creation, and conflation, field asset survey and analysis, large-scale database modeling, distribution network mapping and design, and data warehousing. We work with large utility and telecom organizations throughout the USA. Our team of highly trained and experience engineers and technicians include telecommunications, electrical, mechanical, structural, and civil engineers and technicians.

Our particular competencies—and the source of the highest potential value to the broadband mapping program—lie in the areas of field survey and data verification, database modeling, and telecom experience.

Given below is the list of services, similar to those sought by this RFP, provided by Apex and its partner CSU Foundation to companies in the Utility and Telecom industries.

1) Integrating GPS wireless communications and GIS mapping with a mobile work force management system to provide a complete, turnkey solution for inventorying and mapping Telcom outside plant assets.
2) Developing a telecom data management software and synthesizing engineering data records across a network spanning multiple states.
3) Conducting a comprehensive field inventory of telecom assets throughout a large service territory (project entailed 13 states, in which all COs and RTs across the area were inventoried.)
4) Apex provides services to Fortune 500 companies, leading utilities, government agencies, telecom companies, traditional and electronic publishing companies, and others. We have worked with AT&T, Qwest, Verizon, Thomson Gale, Bowker, National Library of Medicine, National Institutes of Health, and many others.

3.8.1 AT&T U-Verse Project

November 2007 – December 2008
Completed within required timeframe by December 2008

John Audley
C&E OSS Manager
AT&T
Phone: (913) 676-0750
Email: ja0301@att.com

Apex was the project integrator for AT&T's $80 million U-Verse program, widely known as the most critical strategic initiative at AT&T. The project involved six interdependent work streams, including developing a complex data management software, synthesizing data records across multiple disparate databases, performing a comprehensive field inventory of telecom assets throughout the service territory, migrating engineering data to an updated landbase, posting work orders, and cleansing the facilities engineering data.

The field inventory portion of the project was substantial, involving performing field inventory of all central offices (COs) and remote terminals (RTs) across 13 states across. Apex provided an accurate, comprehensive view of the state of its field assets supported by digital imagery and data. By integrating GPS wireless communications and GIS mapping with a mobile work force management system, Apex provided a complete, turnkey solution for inventorying and mapping outside plant assets.

Leveraging digital routing and mapping, GPS and other state-of-the-art technologies Apex's project team worked expertly to:

- capture defined attribute information from the field assets
- document the field and network conditions via digital photos
- record Global Positioning Satellite (GPS) locations
- present it on a Landbase.

3.9 Summary's of Sub Contractor's Work Experience

3.9.1 Gold Country Broadband Demand Aggregation Project

April 2008 – December 2008
Scheduled for Completion in December 2008 and Completed in December 2008

Brent Smith
President and CEO
Sierra Economic Development Corporation
Phone: (530) 823-4703
Fax: (530) 823-4142
Email: brent@sedcorp.biz.

CSU Foundation conducted a survey of Broadband users in the counties of Sierra, Nevada, Placer, and El Dorado in Central California to determine the extent of Broadband penetration as well as the extent of satisfaction with Internet service and support. The results of this survey were mapped to a public web site for review by the program sponsor and by the Internet Service Providers in order to extend areas of Broadband coverage throughout this study region.

This project was part of a larger effort to identify broadband demand and aggregate it for the various Internet Service Providers in the region in order to promote the expansion of Broadband services in the region. This effort was funded by the California Emerging Technology Fund (CETF) as one of a number of similar projects throughout the State of California.

3.9.2 California Demand & Supply Aggregation Mapping

January 2009 – December 2009
Scheduled completion date is December 2009 and this project is currently on track for completion in December 2009.

Gladys Palpallatoc
Associate Vice President
California Emerging Technology Fund (CETF)
Phone: (415) 744-2387
Email: gladys.palpallatoc@cetfund.org.

CSU Research Foundation is identifying the demand for Broadband services and measuring the satisfaction with current Internet access throughout a seven county region in northeastern California including the counties of Modoc, Lassen, Plumas, Butte, Tehama, Shasta, Siskiyou, Glenn, Lake, Colusa, Sutter and Butte. This demand information was mapped to a public web site, and it was then overlaid with an aggregated layer of services provided, identified by type of service, speed, and equipment.

This project both measured and delineated the extent of broadband coverage throughout this region in California. The results of this mapping effort have been used by the California Public Utilities Commission (CPUC) to identify areas of unserved and underserved Broadband coverage as well as to support individual Internet Service Provider applications to USDA and US DOC for BIP and BTOP funding opportunities for Broadband deployment.

3.10 Summary of Bidder's Proposed Personnel/Management Approach

Below please find the proposed team for the State's Broadband Mapping project. A resume for each individual can be found in Appendix D.

Executive Project Manager: Anthony Roberts

The Executive Project Manager for the State's project will be Mr. Anthony (Tony) Roberts. Mr. Roberts is the Director of Operations, Engineering Services at Apex. He is responsible for all engineering solutions projects within the company, which range in size from $5 million to $100 million, and he oversees all of the project managers. Mr. Roberts provides fiduciary and quality management of 1,000 personnel in the USA and India. He has experience developing and managing delivery schedules and project specifications unique to each customer, as well as overseeing multiple vendor contracts with broad interaction schemes.

Database and Solutions Architect: Bill Jamison

Mr. Jamison has more than ten years' experience in Information Systems management and design. He has played diverse roles including Software Engineer, Project Manager, and Business Developer. A key strength is Mr. Jamison's ability to add insight and positive direction to on-going system development efforts by identifying inefficiencies, exploring opportunities, and dramatically reducing costs. Mr. Jamison will be responsible for designing, creating, and managing mapping solutions, workflow tools, and analysis tools.

Technical Leader: Aravind Natarajan

Mr. Aravind Natarajan is the Chief Technology Officer of the Technology Products and Solutions Division at Apex. A 16-year veteran of Apex, he is one of its leading technologists and has experience in strategy, planning, and new product development with industry skills spanning telecommunications, electric and gas utilities, and electronic content solutions. Responsible for many of the innovative technologies developed by Apex over the years, Mr. Natarajan has successfully executed numerous multi-million dollar projects. He has over a decade of experience in managing complex projects and has a strong technical background with experience in software development, requirement analysis, and quality control. Mr. Natarajan will serve as the geospatial subject matter expert and will be responsible for coordinating and managing mapping resources.

Mapping Manager: Prakash Shinde

Mr. Prakash Shinde has a strong background in technical support. Additionally, his responsibilities have included planning, implementing, scheduling, and training, including managing teams of over 150 personnel and communicating directly with the client on system design, specification, and problem resolution. Mr. Shinde will be responsible for managing and directing technical services delivery with specific reference to telecom and GIS.

Systems Integrator/Database Designer: Ratheesh Nair

Mr. Ratheesh Nair is a software engineer with Apex. He has more than eight years experience in designing and developing software and database systems. He has strong background in C/C++, PL/SQL and database design. He has customized Apex's ProField for different projects targeting diverse platforms, according to the client's specifications.

Field Survey Manager: Shane Harrison

Mr. Shane Harrison is a Project Manager at Apex. He has eight years of experience in telecommunications and geospatial engineering. His experience includes managing large teams of company and vendor personnel, allocating work packages to maintain adherence to aggressive schedules, and developing training schedules and safety programs. On this project, Mr. Harrison will be responsible for field verification services and field data collection monitoring and control including schedule adherence.

Chief Technical Consultant: Robert Loube, Ph.D

Dr. Robert Loube has extensive regulatory and legislation experience in the areas of broadband, telecommunications, and related matters of public interest. His broad based experience includes having:

- investigated Verizon Maine's ability to provide broadband services to its customers
- studied demand and supply side dynamics of broadband availability
- analyzed carrier FCC data submissions and pointed out the inconsistencies in the definition of broadband availability
- proposed a broadband deployment plan that would increase the number of broadband rural customers

He specializes in providing technical assistance to state and federal government agencies. Dr. Loube possesses familiarity with the rural incumbent local exchange carriers' customer location databases and exchange maps, and he has examined the cable provider street level maps as a part of his testimony.

Dr. Loube will be responsible for regulatory compliances, including NOFA, NTIA, State agencies reporting, coordination, and demand-side subject matter expertise.

Mapping Services Manager: Cathy Emerson

Ms. Cathy Emerson currently manages two broadband demand and supply aggregation projects in counties located in northern California. Since May, she has facilitated more than a dozen structured meetings and workshops to acquire information from both the end-users and suppliers of broadband. She has facilitated acquisition of maps and shape files of current coverage areas from Internet Service Providers. In this capacity, Ms. Emerson will have Project Management authority over the timely receipt and process of mapping data, correspondence with the various Internet Service Providers to resolve discrepancies and mapping updates, as well as the timely submission of and coordination of the survey results to jump-start the mapping of Nebraska's distribution of Internet services.

Research Designer: Dr. James Fletcher

Dr. James Fletcher's duties have included development of qualitative and quantitative research plans, sampling schemes, questionnaire development, focus group development and management, data collection, data analysis, and report preparation for private for profit businesses, non-profit organizations, and local, state, and federal government agencies. His areas of expertise include survey research methods for telephone, mail, Internet, and in-person survey including survey development, sample design, and control for non-response bias, and data analysis and reporting. During his 32 year career, Dr. Fletcher has completed more than 100 survey research projects that range from local to national in scope. Dr. Fletcher will manage the CSU Foundation data survey design, development, and analysis of the user surveys that will provide the initial picture of Nebraska's distribution of Internet services. Dr. Fletcher's experience with providing similar surveys of this type throughout northern California will allow him to quickly modify and develop a new survey that will target the unique geography and population dispersion in the State of Nebraska.

Web Development Manager: Erik Fintel

Mr. Erik Fintel has developed and maintained parcel base mapping and street level geocoding models for many organizations, including E911 systems. He has extensive experience with database management systems and Geodatabase management and design. Mr. Fintel is part of the GIS team that has been working directly with the California Public Utilities Commission GIS staff to assist with conversion tools and aggregation processes, which included a dynamic coding interface, for updating the California Broadband Task Force Existing Broadband Mapping. For the past 18 months, he has been assisting the GIS team building the data side of a web-based mapping application for California Emerging Technology Fund Aggregate Demand projects. Mr. Fintel will be developing the public interface for the GIS mapping application. This public interface will be distributed via a unique web site in support of the State of Nebraska's and will allow any citizen, ISP, government official, or interested party the ability to query a specific address within the State of Nebraska to determine the availability of providers and publicly available information on speeds and technology of service. Public information will be limited by the degree to which each service providers requires its data to remain proprietary.

3.11 Subcontractors

Below please find required information on Apex's subcontractor on the State's project:

CSU, Chico Research Foundation
Center for Economic Development
35 Main Street
California State University
Chico, CA 95929 0327
Phone: (530) 898-3862\

The subcontractor will provide the following tasks under this RFP:

- Mapping solution architecture and design
- Technical consulting services to align field verification to the NOFA goals
- Geocoding and conflation
- Mapping data aggregation and map creation
- Community outreach and stakeholder development

Apex estimates to subcontract with CSU Foundation for a total of 35% of the project performance hours.

4.0 Technical Approach

4.1 Project Description

Pursuant to the Broadband Data Improvement Act of 2008 and the American Recovery and Reinvestment Act of 2009, the Assistant Secretary of the US Department of Commerce has been required to develop and maintain a comprehensive, interactive and searchable national inventory map of existing broadband service capability and availability in the United States that depicts the geographic extent to which broadband service is deployed and available from a commercial or public provider throughout each state. To this end, the State of Nebraska is seeking to provide its own comprehensive, interactive, and searchable inventory of existing broadband service capability in order to support this Federal requirement.

The State of Nebraska is seeking a contractor that is experienced in collecting and processing broadband mapping data over a wide geographic region, as well as being able to provide that data in a timely manner. Further, this data needs to be made available in a comprehensive, searchable, and interactive manner.

Apex has the right tools, processes, technologies, and manpower required to meet the timelines for expedient delivery of data. As defined in the NOFA (lines 575-576 and 663-664), we will be able to deliver a "substantially complete data set" ready to be filed with the NTIA by no later than February 1, 2010.

Apex's methodology, presented in the Sections that follow, is completely aligned to NTIA's NOFA issued July 2, 2009 as well as the goals of the State. It addresses all the salient requirements of NTIA's NOFA.

Apex understands that the scope of services under this RFP involves submitting a GIS-ready data set containing Broadband service availability data at the service address level from cable, digital subscriber line (DSL), wireless, and applicable other providers. Apex submits to the State of Nebraska that collection of associated Broadband service characteristics at the address level, average revenue per user, pricing, Broadband service provider last mile and middle mile infrastructure data will factor in and conform to the NTIA's clarification to the State Broadband Data Development (SBDD) grant program issued August 07, 2009.

Apex and its subcontractor, the CSU Foundation are uniquely qualified to meet this requirement for the State of Nebraska as will be demonstrated in the following sections of this proposal.

4.1.1 Meeting NTIA's Data and Mapping Submission Requirements

On or before February 1, 2010, Apex will provide an initial set of data to the State of Nebraska. If requested by the State, Apex will provide sample maps in varying media. The interactive maps will represent data that includes, but not limited to:

- Areas of Nebraska unserved by any broadband provider
- Areas of Nebraska served by a single broadband provider
- Areas of Nebraska served by multiple broadband providers
- Locations of towers used to transmit and receive broadband signals

- Actual upstream and downstream transmission speeds at the county level of detail
- Types of technology used to provide broadband services.

Apex will adjust, enhance, improve, modify, or correct the maps as requested by the State. After the maps are approved by the State, Apex will make each map available online on Apex's website dedicated to this project. Users will be able to search through the site by street address.

Apex will comply with all requirements to submit data and maps to the NTIA as announced in the July 1, 2009 NOFA and as specified in the State Broadband Data Improvement Act, and with all requirements to cooperate with NTIA and FCC National Broadband Mapping efforts.

Apex will work to develop, and make available, the market data analysis and maps which can be generated using existing datasets Apex has purchased or those that are made publicly available. These deliverables include county level maps showing the density of households in areas lacking broadband availability.

4.1.2 NTIA's Data and Mapping Submission Requirements

Apex proposes to provide the following deliverables which will conform and meet all the requirements as specified in the NTIA's NOFA and the BDIA with a broader goal of meeting the ARRA objectives.

(i) A substantially complete data set containing data on broadband services based on information from commercial and public sources, web-based information obtained by Apex and Edison Research, augmented with provider supplied data when that data becomes available as of November 1, 2009.

(ii) A substantially complete data set containing data on broadband services based on information from commercial and public sources, web-based information, and survey data obtained by Apex and provider supplied data as of February 1, 2010. The data set will include broadband service availability, weighted average speed, broadband service infrastructure, and community anchor institution tab-delimited text files.

(iii) A complete data set containing data on broadband services by March 1, 2010. All data provided will be accurate as of June 30, 2009. The data set will include broadband service availability, broadband service infrastructure and community anchor institution tab-delimited text files.

(iv) Semi-annual updates of broadband services for five years after the initial data collection.

(v) A state broadband map that can be linked to an existing state website or host a separate website that will be accessible to the public.

(vi) A custom built tool-box and full-feature State website which will have an easy-to-understand interface to allow users to drill down from the State level, through the various geopolitical and census boundaries, down to individual street segments. Users will be able to generate pre-defined reports, construct different views based on service availability, types, and speeds, and perform a variety of on-the-fly queries using the underlying database.

4.1.3 Mapping Website

An important goal of the NTIA's broadband mapping program is to make the State-level map available to the public in a convenient and easy-to-use format. Apex will develop a full-feature State website which will have easy-to-understand interface to allow users to drill down from the State level, through the various geopolitical and census boundaries, down to individual street segments. Users will be able to generate pre-defined reports, construct different views based on service availability, types, and speeds, and perform a variety of on-the-fly queries using the underlying database. Apex will monitor the use patterns regularly and create additional pre-defined reports based on the most frequently performed searches and queries.

4.1.4 Security and Confidentiality

An important goal of the NTIA is ensure both transparency of process and protection of collected data, including Confidential Information.

Apex will work with the State to develop a hierarchical user and associated security model. Established authentication procedures will be deployed from the outset to ensure that qualified users have access to the data as it is compiled on a real-time basis. As mentioned above, users will be able to query the data and display resulting maps freely. In addition, authorized users with sufficient security clearances will be able to drill down into the data to the highest granularity level possible without disclosing confidential data or violating privacy rules established by the State.

Apex will work closely with broadband providers to understand network operations, how data is stored, and gather data relevant to the project goals. We will also work with them to determining the most effective method(s) for sharing and updating data for the next five years, and how non-disclosure agreements should be structured to ensure confidential information is protected while data are effectively translated to accurately represent broadband availability.

Apex will keep the State informed of the providers who have signed a non-disclosure agreement, who have refused, and any other pertinent information. Apex will supply the State with a copy of the non-disclosure agreement that will be used as template for provider administration.

4.1.5 Matching Grants

Item 4b in the section "C. Deliverables" of the RFP states that "The State may terminate the contract, in whole or in part, in the event that the Commission's application for grant funds from the State Broadband Data Development Grant Program is denied or the in-kind state match funding contained in the application for federal funds is rejected by the NTIA." In the event of this happening, Apex is willing to assist the State in raising the 20% grant matching requirement set forth in the State Broadband Data and Development Grant Program NOFA. Apex and its partners together will identify resources, both internal to the team and external resources, to contribute towards the 20% matching funds required for the grant program.

4.1.6 Data Sources

4.1.6.1 Service Provider Data

Apex will develop a comprehensive list of Nebraska facilities-based broadband providers from the list of State Filers made available through FCC Public Notice DA 09-1695 released on July 29, 2009. This list identifies the providers who have made or updated filings through July 9, 2009.

Apex will request information from providers pertaining to speed tiers in their respective service territories. Apex will analyze provider data in association with online speed test data to examine the speed packages offered by providers versus the speed packages to which consumers subscribe. These data can then be compared to consumer survey data in states where Apex conducts residential technology surveys to make assumptions regarding the level of demand that exists for higher speeds in Nebraska. Apex will use speed categories as adopted by the NOFA.

In addition, Apex wishes to make their engineering staff available to smaller broadband providers to assist in the data collection, transfer, and verification process. Apex will assist providers where relevant data is not stored or readily available. Apex will ensure this process is completed in a confidential manner. Such data submitted to Apex by the providers will be normalized, cleansed, and converted into a usable GIS format.

4.1.6.2 External Data Sources

The following are examples of the external data sources that Apes will utilize:

- Apex will gather service provider data from relevant and related sources including but not limited to FCC Form 477 data.
- Cable provider service boundary data and wireless spectrum data will be procured from commercially available sources such as MediaPrints and ComSearch.
- Primary data will be collected from the citizens and communities through online, phone and mailing campaigns conducted as part of Apex's community outreach and field service activities.
- Population and demographic data will be sourced from US Census, InfoUSA, Department of Labor, Department of Education, and US Postal Service.

4.1.6.3 Online Data Collection, Speed Tests and End User Engagement

Apex will develop and launch a website specifically for Nebraska and equip the site with an upstream/downstream speed test tool to measure broadband upload and download speeds at the county level of detail. The site will be available to consumers across the state to test their actual upstream and downstream transmission speeds.

Apex will develop a targeted media campaign to build awareness of consumer's ability to test their broadband speed through the online website that Apex will build for the state consumer speed test site. Following the launch, Apex and State will jointly determine whether there are other reasonable outreach measures that can be taken to increase the number of speed tests, either statewide or within certain counties, if numbers are lower than necessary for statistically relevant reporting.

4.1.7 Marketing and Communications Strategy

Apex, in association with CSU Foundation, is proposing a unique and effective Collaborative Efforts mechanism (section 4.2.8) and a broad-based Community Outreach strategy called *NetSpeed* (section 4.2.11), which present ample opportunities and an excellent platform for implementing the marketing and communications part of the project.

4.2 Scope of Work

Apex's approach and methodology, presented below, is aligned to NTIA's NOFA issued July 2, 2009 for the State Broadband Data and Development Grant Program. It addresses the salient requirements of the NOFA in order to facilitate grant preparation and to maximize the potential for award.

Apex's overall methodology is designed to ensure that the services are provided in a timely, cost-effective manner. The methodology combines provider-submitted data with commercial and public data. This combination provides flexibility in obtaining and utilizing various data sources, avoids total reliance on provider information that may be incomplete, and increases the accuracy of the mapping initiative. The methodology will allow the project team to:

- create a geographic statewide map of "wired" and "wireless" broadband service to identify where there is current broadband service and the types of infrastructure used to provide broadband service by street segment.
- identify census blocks and contiguous groups of census blocks that are unserved or underserved.
- determine the demand side factors and barriers to broadband adoption at the census block level.
- fulfill the NTIA's data and mapping submission requirements.
- provide the State and other state agencies with a custom built tool-box to perform with the software platform designated by the State. The tool-box will allow the State to run queries on the data base and generate additional maps.

Apex's methodology has the following main components:

1. Broadband service availability data made available at the census block level for census blocks which are less than two square miles in area. For Census blocks larger than a

two square mile area, field-verified and validated broadband availability data will be collected, aggregated, and verified at the street segment level.

2. Service Provider speed tier data including the wireless tower and coverage area data obtained through field verification and data collection through drive testing, spectrum analysis, and wireless propagation.
3. Commercial street-level base maps with geo-coded addresses of business, and community anchor organization augmented by field verification and stratified survey sampling (statistically significant).
4. Deploying ProField™, Apex's proprietary field inventory, data collection, and verification platform. ProField is a powerful Web-based workflow application that coordinates broadband mapping activities over large geographic areas. The application supports an innovative approach to broadband data collection and verification that combines existing GIS data, broadband supplier data, call center queries, online surveys, and the deployment of mobile verification teams to conduct spectrum analysis for wireless connectivity.
5. Calling and direct mail campaigns, phone interviews, and online contributions by communities and participating citizens.
6. Web-based application for Service Providers to verify/validate their service areas.

4.2.1 Base Map Creation

Apex will derive synergies by using commercial and public data, which will be immediately geo-coded onto street map data and used to compute a "base" maps along street segments. The street segments will be defined by E911 road segments. The E911 road segments will be compared to commercially available street maps to ensure complete coverage in each Census Block. As provider data becomes available, the provider, commercial, and public data will be merged. Data validation and cleansing procedures perfected by Apex's subcontractor over the past 20 years will be applied to improve the quality and reliability of the data so that "best" data from all sources are retained in the database. Some examples include conflating customer service location and billing address; matching and correcting facility location addresses; and applying adjacency and continuity logic to close data gaps, etc.

To determine broadband availability, Apex will develop an adaptable program that queries provider web sites. The program will enter customer addresses and retrieve information regarding broadband availability at those addresses. Apex will work with the providers to ensure that the providers do not shut down their web sites due to the large volume of requests and to ensure that the program is activated only during extreme off-peak periods of the day. This process will allow Apex to generate provisional substantially complete data by the NTIA's preferred date of November 1, 2009. When carriers provide data on service availability from their internal databases, the two data sources will be compared to validate the broadband availability information. Additional validation processes will be developed as part of Apex's Field Survey and Customer Outreach Program; see Section 4.2.3. The "base" broadband availability map combines the customer location data with the broadband availability data.

4.2.1.1 Identifying Unserved Areas

The customer location data and broadband availability data will be combined at the Census Block level to determine those Census Blocks or groups of contiguous Census Blocks where 90 percent of the households lack access to facilities-based broadband service, and therefore, are unserved areas.

4.2.1.2 Identifying Underserved Areas

The following will be performed to identify underserved areas:

a) Facilities: The customer location data and broadband availability data will be combined to determine those Census Blocks or groups of contiguous Census Blocks where no more than 50 percent of the households have access to facilities-based broadband service, and therefore, are underserved areas.

b) Advertising: The web sites of every wireless broadband provider will be examined to determine whether the provider is advertising broadband transmission speeds of at least three megabits per second in the area. If not, then the area will be designated underserved.

c) Subscription: Provider data on broadband subscribership will be aggregated across all providers to determine if at least 40 percent of the households subscribe to broadband service. If this condition is not true, then the area will be designated underserved.

4.2.1.3 Local Exchange Providers

Local exchange providers' service territories and exchange boundaries will be layered onto the street maps and combined with customer location data and service availability data to generate a broadband availability map for each local exchange provider.

In addition, local exchange provider central office and remote terminal locations can be used to verify broadband availability. In general, the industry uses either a 12,000 foot or an 18,000 foot maximum copper loop to determine if a customer can obtain DSL service at 768 kbps per second downstream. These engineering practices are dependent on the location and length of bridge tabs and the types of plug-in cards used to provide DSL service. Apex will construct polygons around each central office and remote terminal that ensure that the road distance from the end-user to the termination point is no greater than 12,000 (18,000) feet. Apex would remove a broadband availability designation from any location that is greater than 18,000 feet from a termination point. Locations between 12,000 and 18,000 would retain their broadband availability designation only if Apex can verify that broadband service is available at those locations from two other sources.

4.2.1.4 Cable Providers

Commercial boundary data and information on the number of homes passed by the cable plant and the number of households in the franchise area will be used to develop the initial base map. Broadband availability and subscribership data are available on a franchise basis. Data obtained from provider web sites will be used to determine broadband availability at the street level and by Census Block. The web-based data will also be used to verify the franchise level availability and subscriber data. In addition, as providers submit internally generated data, information from all data sources will be compared and reconciled.

4.2.1.5 Wireless Providers

1) Collect service provider data on facilities-based providers of wireless broadband service that is not address specific (e.g., nomadic, terrestrial mobile wireless, or satellite) as required in the NOFA (Technical Appendix, "Broadband Service Infrastructure in Provider's Service Area")
2) Research FCC license and tower database, internal wireless carrier databases and other industry resources, produce tabular results by frequency/owner
3) Perform drive testing and service verification:
    a) Drive Test major roads and communities in and around the desired service area for coverage within the areas.
    b) Collect RSSI (signal strength) measurements for as many of the in service operating Wireless Carriers as possible including: Nextel, Cellular A Band, Cellular B Band, and Broadband PCS A – F Carriers.
    c) Process the data and provide copies of the plots depicting the coverage for each Wireless Carrier for inclusion in the application.
4) Develop coverage maps for each identified carrier, review appropriate terrain and best land use data, develop link budgets for each site and network, analyze and adjust predictions as necessary
5) Provide data in GIS-compatible map layers depicting areas in which broadband service is available to end users with map areas being closed, non-overlapping polygons with a single, unique identifier for Service Providers to verify/validate their service areas.

4.2.2 Accuracy and Verification

4.2.2.1 Validation by Service Providers

The base maps developed above will be made available to Service Providers via a secure web application for a defined period of time. Each Service Provider will be able to interactively validate the base maps including speeds, service types, and technology/equipment details in their service area and make necessary corrections.

All changes will be audited by Apex and, if necessary, follow-up calls will be made to the Service Provider.

4.2.2.2 Validation by End-users

Apex will develop a website in which an end-user can enter their address and broadband availability and speed at their location. The website will automatically compute the actual upload and download speeds of the connection.

A direct mailing campaign will inform end-users of the availability of the website.

4.2.2.3 Broadband Confidence Ranking

Using an algorithm based on Broadband Service Provider (BSP) exports, census data, and contiguous demographic clusters, we are able to focus verification efforts on areas of low confidence. Confidence levels are enhanced by analyzing overlapping BSP coverage area claims and demographic data such as population, income, and education levels. The ranking is further influenced by independent verification methods such as direct mail, online and telephone surveys, and mobile field inspection.

By focusing on areas of low confidence, data quality is maximized while reducing costs associated with verification activities. Emphasis will be placed on rural areas, on areas near service territory boundaries, and on areas near the boundaries of engineering constraints. Anomalies identified by the system are submitted to each BSP for clarification and are confirmed or rejected by independent verification techniques listed below:

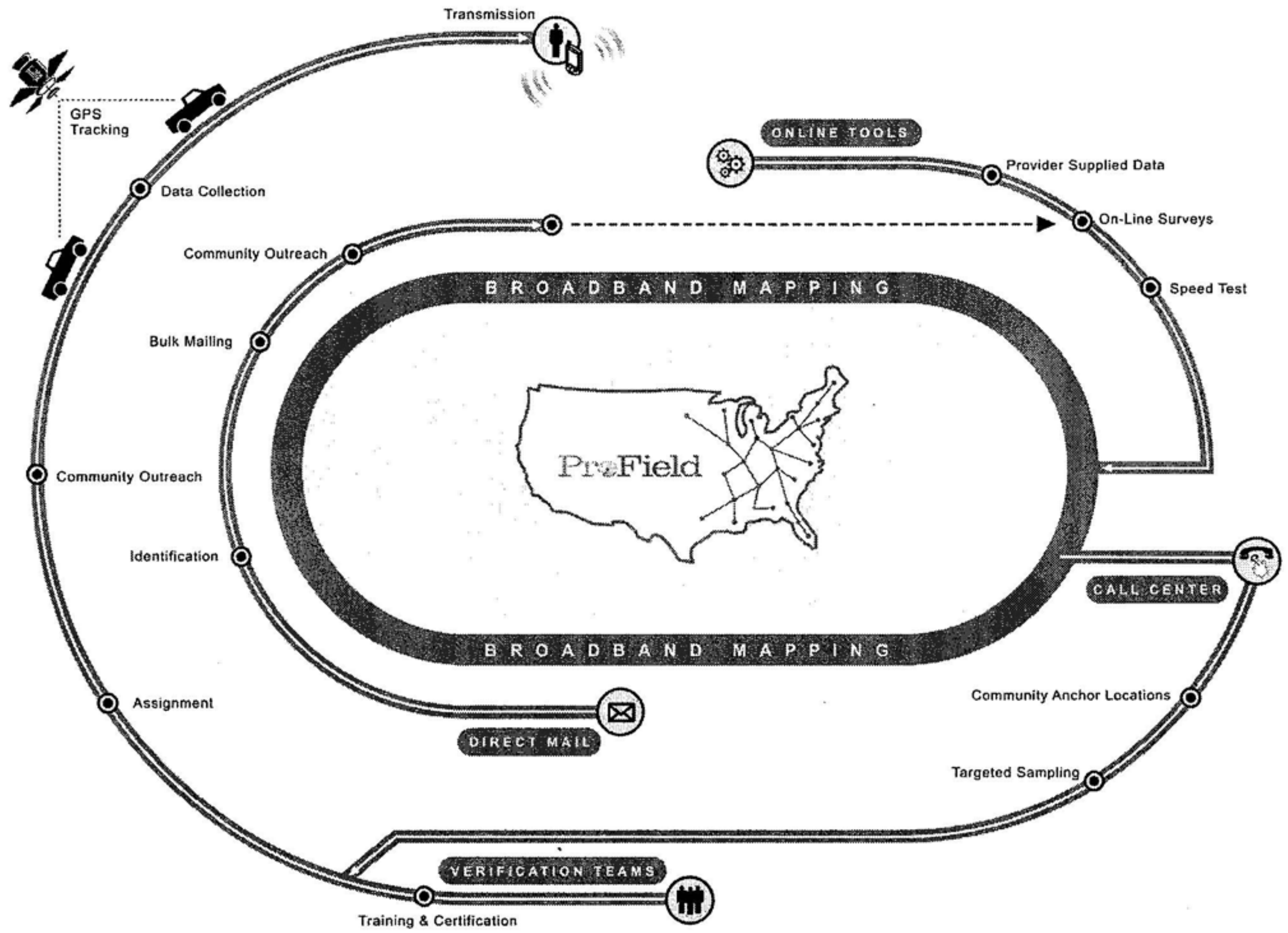
- Direct Mail
- Online Survey Systems and Speed Tests
- Call Center
- Mobile Verification Teams

System support and problem escalation is handled through ProField's embedded ticketing system which allows survey technicians and other support staff to post questions and issues online and have those questions routed to appropriate response teams.

ProField provides the ability to create custom drill down reports to present the data collected and verified from the field. These reports can be used to monitor, direct and control the field data collection and verification activities. All reports can be exported to Excel for further manipulation.

The ProField workflow process is illustrated in Figure 1.

Figure 1: ProField Workflow



ProField consists of the following components and interfaces to facilitate broadband inventory collection.

- Hosting / staging provider supplied data
- Field workforce management
- Support for Call Center activities
- Community outreach
- Integration with GIS mapping software

The broadband mapping initiative will begin by collecting and importing web-based and commercially available data along with provider-supplied data into a database staging area, as the provider data becomes available. While in the staging area, data will undergo consistency and attribute checks to determine transformation requirements and corrections need to be made before it is migrated to the production database tables.

Figure 2, Figure 3, and Figure 4 below are examples of service availability maps that can be generated on the mapping website.

Figure 2: Service Area Polygons

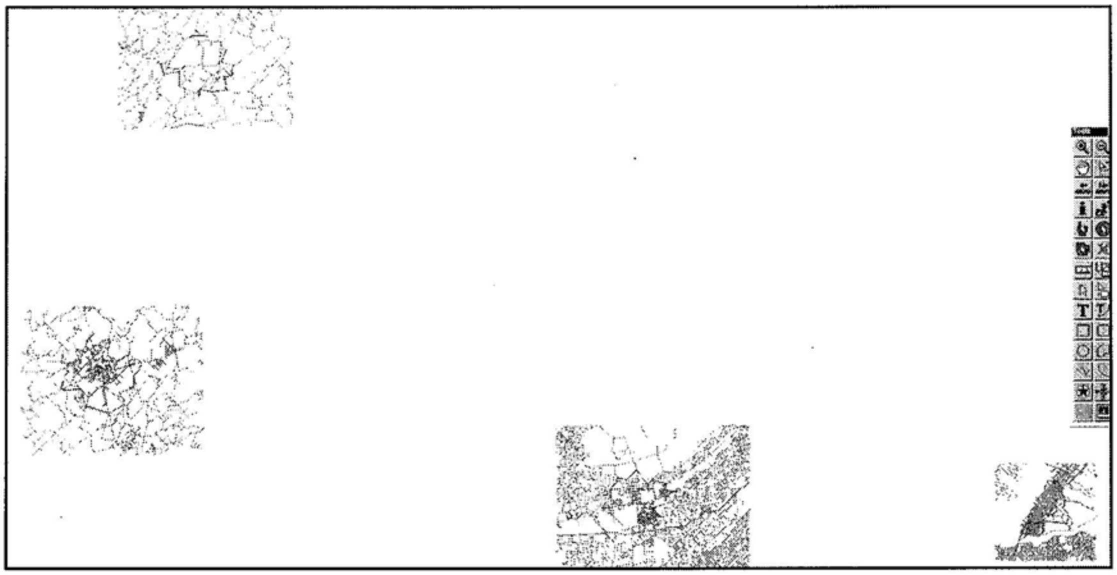


Figure 3: Types of Service Available by Road Segments

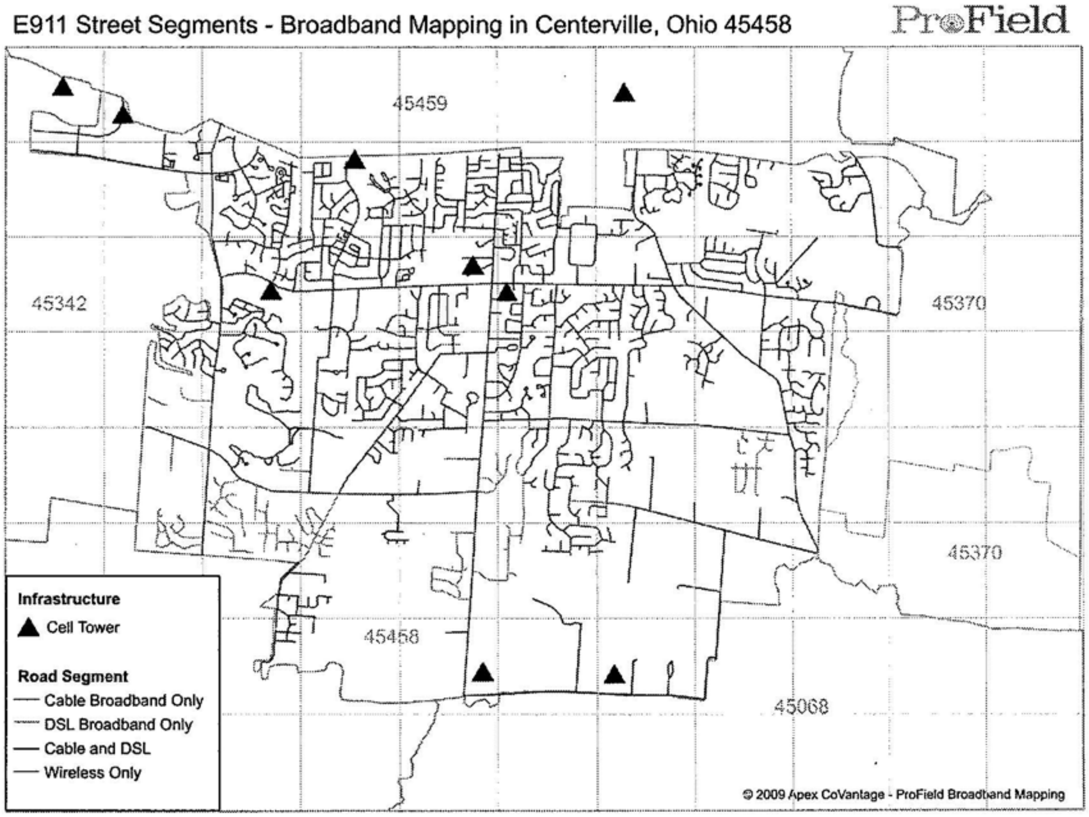
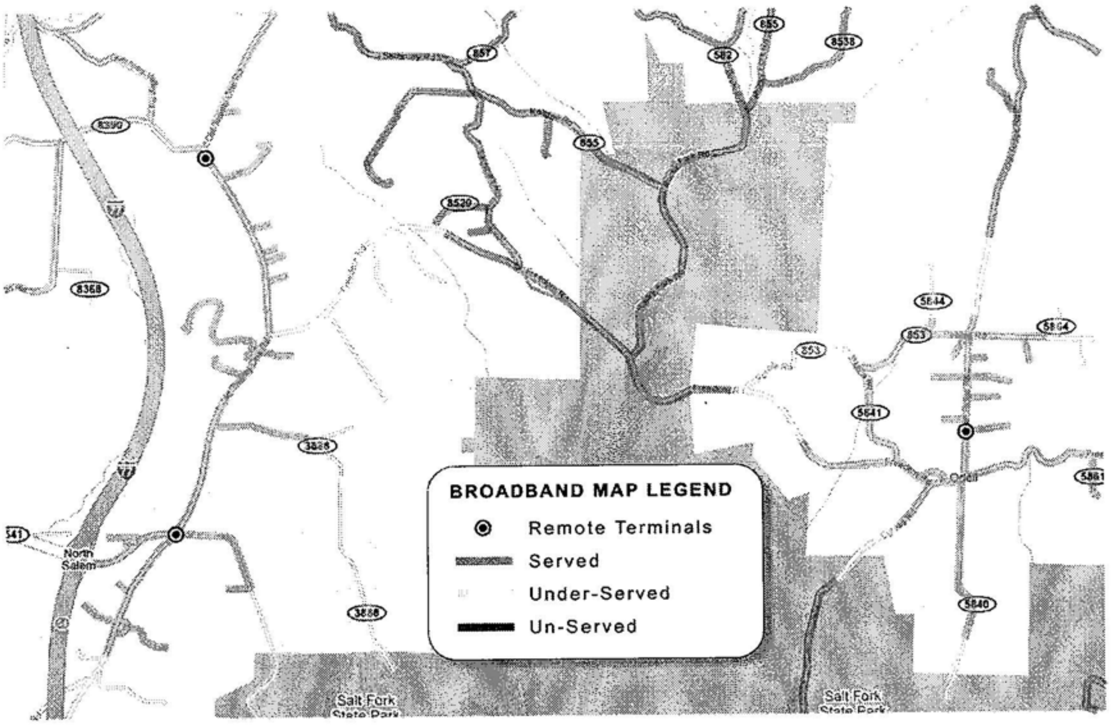


Figure 4: Dynamically Generated Representation of Unserved, Underserved, and Served Areas



4.2.3 Field Verification and Community Outreach

Apex will deploy its ProField software platform to conduct a field verification of broadband availability based on a sample of locations augmented by mail and telephone surveys. Our field technicians will take readings of wireless bandwidth in the area. The field technicians will perform sample inspections of telephone and cable plants to verify remote terminal and cable hub locations.

Apex's field verification and community outreach program will be integrated through use of Apex's ProField software management tool.

4.2.3.1 Field Verification Methodology (Statistical)

Edison Research will conduct the verification and field survey within a statistically significant size of census blocks in the state that are selected to arrive at an anticipated margin of error of ± 5 (with 93% confidence).

Within each census block, sample households, community anchor institutions, and businesses will be sampled to ensure coverage. The random sample will be stratified geographically (e.g. rural/non-rural) and demographically. Sample size allocation procedures will be used to determine the appropriate number of census blocks for rural and non-rural areas.

Missing census blocks will be imputed and estimated using hot-deck imputation methods. Edison Research will incorporate a dynamic learning model to establish a decision rule to impute and estimate census blocks. Statistical techniques will be used to estimate the missing census blocks.

Missing census blocks will be estimated using methods such as multivariate cluster analysis, maximum likelihood, and Bayesian modeling for missing data. The sampling model employed will include age, race, sex, education, income, topology, household density, and size of census block.

Once the state has been sampled, the model will be implemented in such a way that additional samples can be taken and combined with any previously collected data. For ongoing updates, Edison will sample from new service providers entering the market and additional facilities created by existing providers.

4.2.3.2 Field Verification Execution

Apex and CSU Foundation will hire, train, and certify a team of interviewers to be deployed in the field for conducting field verification, data collection, and community outreach activities. Apex will deploy and customize its field data collection and verification platform ProField and the associated GPS handheld devices used for data collection and reporting from the field.

Interviewers will be assigned specific census blocks to cover throughout the state. When interviewers arrive in a census block, they will be given a procedure to randomly select street segments to conduct face-to-face interviews.

Once an address range on a street segment is selected and the interviewer has cooperation from a head of household or community anchor location or a business, the interviewer will collect the information pertaining to demographics, availability of broadband service in the area, awareness of broadband availability, adoption trends, barriers to adoption, etc.

Locations with Service

Following the face-to-face interview, in the locations where broadband service is available and adopted, the interviewer will give a unique ID to the respondent and encourage him/her to run a speed test on the designated website. This ID will help automatically log the connection speed for that address.

Locations without a Service

The interviewer will deliver information on the benefits of broadband and the ability to check availability on service provider Web sites. After the completion of every face-to-face interview, the interviewer will take a wireless bandwidth reading of location.

Usage of handheld GPS devices equipped with ProField software will have the following benefits to the data collection and verification activity:

GPS device allows confirmation of interviewer location.

Wireless bandwidth readings and face-to-face interviews are immediately sent to a central location for processing.

Data will be continually added to the Apex mapping model to adjust the geographic broadband service map and will provide additional information on other census blocks that should be sampled for field verification.

4.2.4 Final Deliverable

On or before March 1, 2009, Apex commits to provide the final deliverable which includes a field verified/validated, geo-coded interactive map that represents the collected data. This broadband service availability map website can be linked to an existing state website or hosted separately that will be accessible to the public. The map will be searchable by street segment and, to the extent possible, provide the type of technology, speed tiers, and number of providers available. For providers of wireless broadband, the spectrum used for the provision of service will be supplied. Apex will include the findings from its field survey into the map so as to depict the broadband availability versus the actual adoption rates at the census block level.

The deliverable will include data representing:

i. geographic areas in which broadband service is available;

ii. technologies used to provide broadband service;

iii. spectrum used for the provision of wireless broadband service in such areas;

iv. the speeds at which broadband service is available;

v. broadband service availability at Community Anchor locations including public schools, libraries, hospitals, colleges and universities, etc.

Apex in addition is willing to provide a custom built tool-box and full-feature State website which will have an easy-to-understand interface to allow users to drill down from the State level, through the various geopolitical and census boundaries, down to individual street segments. Users will be able to generate pre-defined reports, construct different views based on service availability, types, and speeds, and perform a variety of on-the-fly queries using the underlying database.

Apex understands the scope of services require providing semi-annual data updates to the final map. The updates for data as of December 31, 2009 and as of June 30, 2010 will be submitted to the State of Nebraska prior to September 1, 2010. Additional updates will be prepared and submitted to the Sate of Nebraska in timely fashion so that it can meet the NTIA deadlines.

After the initial delivery of the broadband availability data and further to the hosting of a completed Broadband Map website, Apex will continue a semi-annual version of the broadband data collection including field data sampling, telephone surveys, and mailing surveys as required by the NTIA's NOFA. Apex will deploy and use its ProField data management software for this purpose.

4.2.5 Sustainable Framework for Data Upgrading

Apex will provide semi-annual data updates to the State for submission to the NTIA. The updates for data as of December 31, 2009 and as of June 30, 2010 will be submitted to the State prior to September 1, 2010 so that the State can forward the data to the NTIA by September 1. Additional updates will be prepared and submitted to the State in timely fashion so that it can meet the NTIA deadlines.

Apex will establish a secure web site that will allow broadband providers to upload data files. The web site will contain authentication procedures that would prevent a provider from viewing the data of another provider and would also prevent other non-qualified individuals from viewing or obtaining any of the data.

After the initial delivery of the broadband availability data and further to the hosting of a completed Broadband Map website, Apex will continue a semi-annual version of the broadband data collection including field data sampling, telephone surveys, and mailing surveys as required by the NTIA's NOFA. Apex will deploy and use its ProField data management software for this purpose.

4.2.6 Updating Provider Data

Apex will translate provider data into a preliminary representation of broadband availability for each provider's service area. Apex will work directly with providers through a confidential iterative process whereby the preliminary maps are refined until both Apex and the provider believe the maps are accurate. Apex will be responsible for data gathering and relationship building with providers, and for transition and analysis of the data. This process will include constructing engineering and wireless propagation studies, developing GIS datasets, and analyzing data to develop the corresponding demographic map components.

Apex will process provider datasets as received by November 1, 2009. To the extent possible, provider data will be continued to be solicited, gathered, and processed after this date for inclusion in a final mapping data deliverable. The final mapping data deliverable will attempt to represent at least 95% of the broadband coverage within the state. Apex will create a structure and communication protocol targeted to elicit a 100% response rate from all facilities-based providers for the project.

Apex will make final modifications to the maps based on a field verification process with providers and as requested by State.

4.2.7 Ongoing Support and Maintenance

Apex will include information on how the public can provide feedback, report inaccuracies, and ask questions about the maps directly on their website. Resources will include, but not be limited to, a direct online form, a toll-free telephone number, and e-mail communications options. Apex will investigate inaccuracies reported by the public with the appropriate broadband provider. Adjustments to the maps will be made as appropriate.

Apex will continue to host the maps and online interactive (searchable) version of the maps on its website for the first two years and through the years 3 to 5 as may be mutually agreed upon by the Parties, or until such time as the State of Nebraska may engage another broadband mapping provider for purposes substantially similar to those outlined in the Contract.

4.2.8 Partnership Development/Stakeholder Management

Apex, in association with its non-profit partner CSU Foundation, will collaborate with state agencies to help them enhance the existing maps and to verify the data that the state agencies have or will collect. Apex will also identify and work with state and local technology planning teams along with broadband providers in an effort to reach customers in unserved and underserved areas. If planning teams are not currently engaged, Apex will initiate a process of forming such teams by working with economic development agencies, local technology firms, schools, and universities. Through these collaborative efforts, Apex will support efforts to enhance computer ownership, to facilitate information exchange regarding the use and demand for broadband services, and to aid entities applying for broadband grants.

As a part of its work efforts over the past 18 months in support of a variety of initiatives in the State of California, the CSU Foundation has facilitated a public/private partnership with all the appropriate Stakeholders in an effort to provide a collaborative approach to Broadband development. Through over 26 county meetings attended by county and municipal elected and administrative leaders, Internet Service providers (both wireline and wireless), key anchor institutions (K-12 schools, libraries, medical and healthcare institutions, public safety officials, community colleges, and universities (both public and private). These meetings have resulted in the key stakeholders knowing the major technical, administrative, and regulatory issues facing the community that can either inhibit or promote the spread of broadband in their communities. As a result, CSU Foundation has developed a methodology for gaining the trust and confidence of these key stakeholders – particularly the Internet service providers such that when the data call went out to provide coverage maps in support of CPUC requirements, the CSU Foundation was able to quickly obtain and process over 200 maps of coverage areas.

By engaging this broad segment of stakeholder groups, the CSU Foundation has a track record and a history of quickly garnering and maintaining support from the service providers as well as from the state organizations that need to rely on this provider data.

Apex, in collaboration with CSU Foundation, proposes to work as a bridge between the user community and State to coordinate the efforts of bringing broadband access to the unserved and underserved areas of the State. Apex will work with the State and existing stakeholders who are already developing infrastructure, to collaborate and provide support for the community outreach efforts planned to reach more people in a shorter period of time, thereby encouraging increased adoption rates.

4.2.9 Public- Private Partnership

Attracting private contributions and creating a sustainable public-private participation structure is central to the expansion of broadband networks. Apex's team will work with small services providers in an inclusive manner to plan region/community-specific broadband adoption and planning programs aimed at increasing computer ownership, creating higher demand, and leading to increased adoption rates. Conscious efforts and planned programs will be designed in consultation with the State and rolled out on a pre-agreed priority basis to focus specifically on the unserved and rural communities.

4.2.10 Demand Creation

Apex proposes to encourage public participation right from the start of the mapping efforts. Apex's field data collection and verification methodology includes planned methods aimed at encouraging the public and communities to take ownership and participate in the mapping program by sharing their insights and availability information, thereby creating an ongoing engagement. Literature aimed at increasing awareness and creation will be made available to the communities, and people will be incentivized to participate and contribute to this program.

Note: Apex seeks to complement the role of the State, service providers, and infrastructure developers to make broadband service to a larger population in the State of Nebraska.

4.2.11 Apex *NetSpeed* Community Outreach Program

Apex's *"NetSpeed"* program is designed to the State's mission to promote the adoption of broadband service throughout unserved and underserved areas.

NetSpeed's mission is to increase broadband adoption rates and implement community outreach and planning programs prioritized by Sate of Nebraska. *NetSpeed* will work with the State and community anchor locations to develop and execute efforts to achieve the goals of the State's Broadband Data Development and Mapping initiative.

In consultation with the State and *NetSpeed*, Apex will craft a vision statement and marshal Apex's internal Marketing Team and PR resources to run through the duration of the program. Apex will use a mix of media and channels including planned outreach events, press releases, and community anchor outreach programs to further the mission and goal of increasing broadband adoption rates in the State.

Working closely with State, Apex commits to develop a comprehensive marketing and communication strategy aimed at promoting statewide broadband adoption/deployment. Apex has over 15 year of experience in creating and executing National and International Branding strategies to promote adoption of new technologies and services.

Apex would draw substantially from its past experience of conceptualizing and articulating a value message to the community and public at large. Apex's involvement for the past 20 years with grass root level organizations and contribution to various communities across the USA and the world has given us the required insights to strategically approach the communication aspect.

4.3 Nondisclosure Agreement

An important goal of the NTIA is ensure both transparency of process and protection of collected data, including Confidential Information.

Apex will work with the State to develop a hierarchical user and associated security model. Established authentication procedures will be deployed from the outset to ensure that qualified users have access to the data as it is compiled on a real-time basis. As mentioned above, users will be able to query the data and display resulting maps freely. In addition, authorized users with sufficient security clearances will be able to drill down into the data to the highest granularity level possible without disclosing confidential data or violating privacy rules established by the State.

Apex will work closely with broadband providers to understand network operations, how data is stored, and gather data relevant to the project goals. We will also work with them to determining the most effective method(s) for sharing and updating data for the next five years, and how non-disclosure agreements should be structured to ensure confidential information is protected while data are effectively translated to accurately represent broadband availability.

Apex will keep the State informed of the providers who have signed a non-disclosure agreement, who have refused, and any other pertinent information. In Appendix B, please find a copy of the non-disclosure agreement that will be used as a template for the protection of the confidential data collected from providers.

4.4 Technical Considerations

Apex will provide a final set of maps to the State at the end of the project; Apex will also provide the "shape" files associated with the broadband mapping that are ArcGIS compatible, delineate between where broadband is provided and is not, and are an aggregation of all providers participating in the Nebraska mapping initiative. These "shape" files will accompany other supporting files to enable editing of the data, exclusive of any provider-specific information.

Apex proposes to deliver the GIS layered map of the current infrastructure in a form compatible with both ESRI and Google Earth Visualization Platform, which when hosted on the website can be viewed on equipment without GIS software. The intent of this deliverable is to satisfy the requirements of the NOFA and the BDIA. This will be a working geodatabase with all of the source data layers, relationship classes, and references used to process the street centerline deliverable. The intent of this deliverable is to minimize the sustainability effort for annual updates of any of the source data layers, suitable for users with advanced GIS skills.

The map will be searchable by street segment and, to the extent possible, provide the type of technology, speed tiers, and number of providers available. For providers of wireless broadband, the spectrum used for the provision of service will be supplied. Apex will include the findings from its field survey into the map so as to depict the broadband availability versus the actual adoption rates at the census block level.

The deliverable will include data representing

(i) geographic areas in which broadband service is available;
(ii) technologies used to provide broadband service;
(iii) spectrum used for the provision of wireless broadband service in such areas;
(iv) the speeds at which broadband service is available;
(v) broadband service availability at Community Anchor locations including public schools, libraries, hospitals, colleges and universities, etc.

To achieve the above said objective, Apex will deploy CSU Foundation's experience with the mapping of Broadband supply and demand for the State of California for the past year. In this time, a formal process has been developed that will deliver quality mapping of broadband demand information as well as broadband supply (coverage areas) in a timely and accurate manner. This process can cost effectively be replicated for any state or throughout any region of the country. Further, this work is not a once-and-done approach, but provides clients the capability and tools to accurately assess the state of broadband deployment well into the future. A graphic of our Broadband Mapping Functions is provided in Figure 6 on page 4-22.

Accuracy of mapping information is paramount to effectively managing the deployment of high speed Internet. Working with State Geographic Information System (GIS) offices or with County GIS departments, the CSU Foundation process starts with the collection of parcel data (shape files and reference information) for each physical location within the state (*Process Item A*). Additionally, CSU Foundation will request a state-wide database of address information (*Process Item B*). This data is needed to develop the underlying layers of the map that will ultimately be created and will be used as reference information for the accurate geocoding of broadband demand and supply data. Where such information may not be readily available, CSU Foundation can utilize commercially available but potentially less accurate reference information.

CSU Foundation has also built a database of reference information from a variety of public sources (*Process Item C*) including census, demographic, imagery, elevation, transportation, populated places, hydrology, political boundaries, and public infrastructure. These data will form various layers of a computer-based map of the state or region. An example of a Geographic Information System's Data Layers is shown below in Figure 5.

Based upon any set of criteria that is provided by the state or the region, CSU Foundation will develop unique data layers that can be overlain the geographic territory (*Process Item D*). For example, if there are specific rules regarding what is a rural area versus an urban area (non-rural), or what is a remote area versus a non-remote area as in the current Broadband Mapping NOFA, these can be segmented and used to extract additional information from the base map layers, e.g. population, census blocks, Congressional districts, and the like.

Concurrent with the collection of parcel, address, topographic and base layers of information, Apex will contact the various providers of Internet services that exist in the State or region. Working in concert with or on behalf the client, Apex will solicit coverage maps from each provider (*Process Item E*). Where the provider does not have the technical capability to provide a coverage map, a relatively simple process and toolset can be provided to the service provider with instructions on how to generate a coverage map using free versions of Google Earth. Additionally, CSU Foundation will obtain information on the current infrastructure used by the various providers of Internet services including physical locations of Digital Subscriber Line (DSL) Central Offices (CO), Wireless Towers, Wireless Radio Transmitters and Types, Fiber Lines, Digital Cable runs, etc. (*Process Item F*).

As a part of our Project Management Services, Apex will impress upon the service providers that it is in their interest to provide accurate maps of their coverage areas as this data can and will be used by the public to identify potential sources of broadband services (*Process Item G*). Failure to deliver service in an area previously identified by a provider can result in adverse publicity, but the ability to provide accurate mapping can result in new leads and potentially additional subscribers of broadband service.

As data is collected, it will be built into separate layers within our GIS application (*Process Item I*), and an on-line capability will be developed and made available via a public web site to display this information in an interactive environment (*Process Item J*). Users of the system will be able to query the system through a variety of included toolsets that will allow them to:

- Look-up specific addresses
- Identify broadband services by
  - Type
  - Speed
  - Equipment type
- Identify broadband carrier and their contact information
- Provide a comment block to capture individual public input
- Provide a publicly available broadband connection speed test
- Identify Census-based data and data boundaries
- Call up specific survey-related data queries
- Print the results of various mapping layers to a local printer
- Provide a "Locate" Tool that will identify the Broadband coverages and speeds by provider for any specific geographic location within the study area

Finally, Apex will promote the program and the public involvement through a series of outreach events and workshops, as well as through an on-line tutorial as explained in (*Process Item G*) and in Section 4.2.8 . These promotional events are important in order to obtain community buy-in for the development of a sustainable adoption strategy involving key business activities, community anchor institutions, critical community facilities, public computing centers, and household users of broadband services.

An important part of this effort will be to collect feedback and input from individual users of the on-line GIS web site (*Process Item K*). This continuing feedback will reinforce the need for additional broadband services and will provide feedback to the state, the region, and to the providers of where there is an ongoing demand for broadband services that can be continued indefinitely.

Figure 5: Example of GIS Data Layers

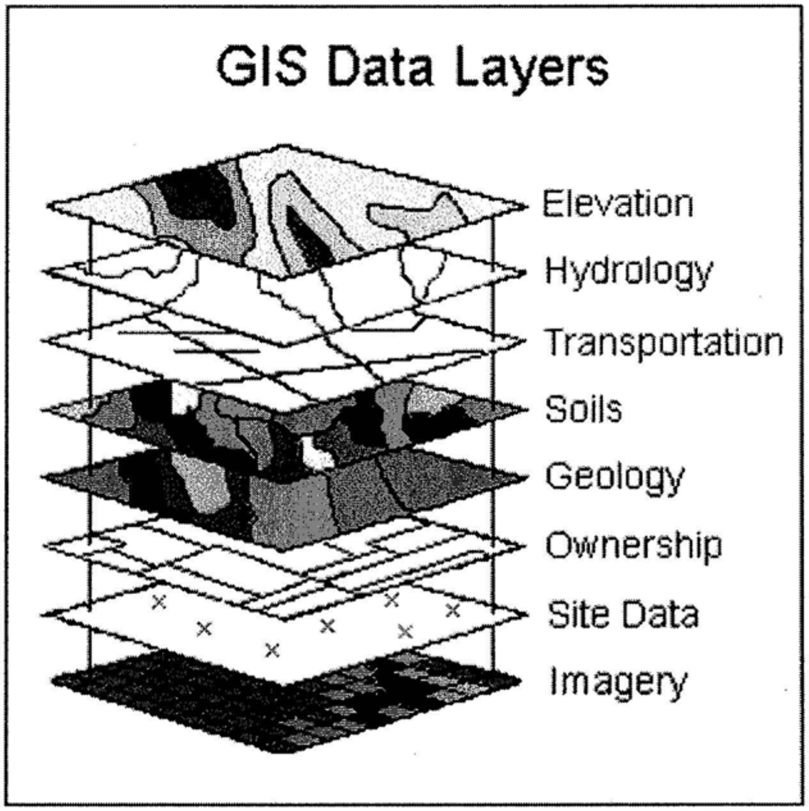
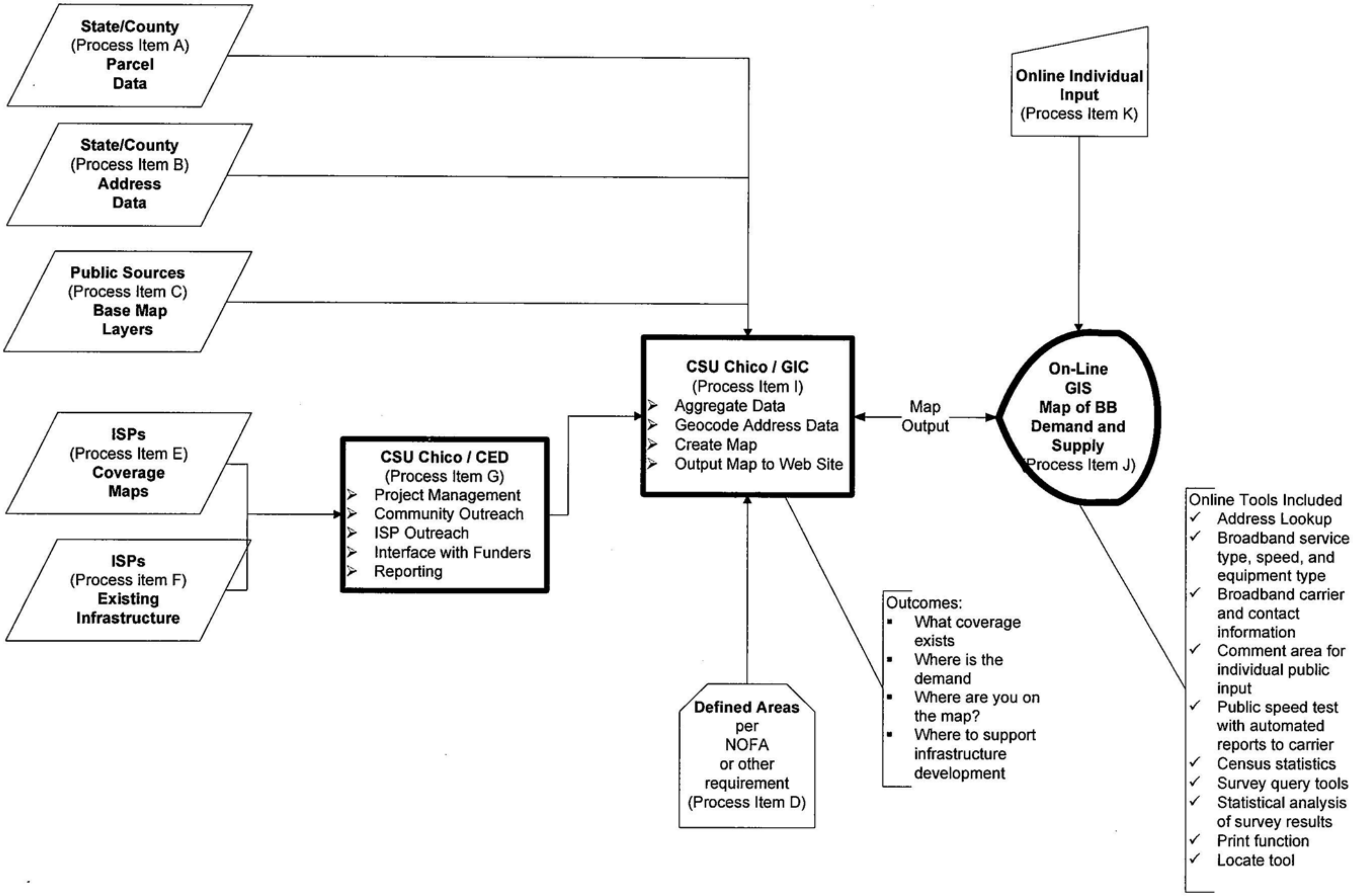


Figure 6: Broadband Mapping Functions



4.4.1 Benefits

By using mapping resources from the State and/or region, the Broadband mapping application can be maintained at a level consistent with other State or regional data sets. This precludes having to recode and normalize the data if used for other applications.

The process provides a kick-start for identifying broadband demand without having to do door-to-door interviews, which is an expensive and labor intensive process that ends up yielding highly questionable survey results. Modern statistical survey techniques can provide significant insight into the demand for broadband services while screening for such factors as age, sex, and occupation that may skew other results.

Apex's technology partner CSU Foundation has successfully employed this approach in Northern California under the auspices of the California Public Utility Commission and the California Emerging Technology Fund, and used these results for applications by Internet Service Providers for Broadband funding from the Federal Government.

Apex in association with CSU Foundation proposes a complete and fully tested process that can be implemented immediately for any Broadband mapping application. By using an on-line GIS capability, the State or region is provided full visibility and transparency of effort. Service providers can use the data to target new service areas, the public at large can interact with the application to provide continuing and updated information on desired service, and governments can use the system to target incentives for the expansion of broadband services into an unserved or underserved region.

Complete coverage area down to the individual address level is provided for in this approach. Once collected at this level, data can be aggregated to higher levels of abstraction (including Census Block, Block Group, Tract, Zip Code, County, etc.) to support a variety of purposes and reporting requirements.

4.4.2 Hardware Architecture

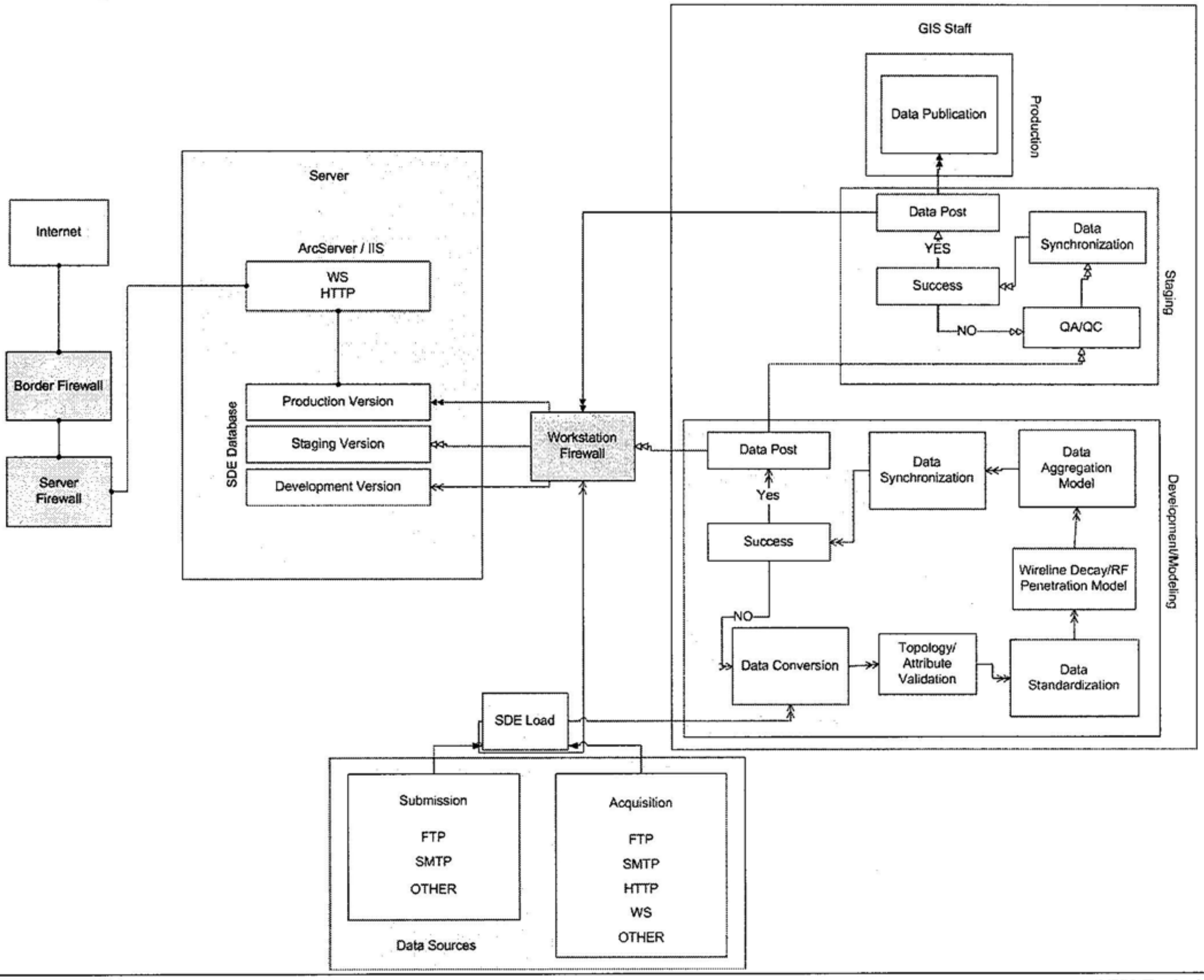
Figure 7 details workflow and network design that will be employed by the CSU Foundation to support the State of Nebraska. ArcGIS servers are being used because they are the industry standard for GIS software. This software is needed for online deployment of broadband data maps. Further, this hardware and software combination can be used for creation of other mapping related documents including spreadsheets, queries, reports and charts. These servers carry with them inherent maintenance, backup, security, and licensing costs borne within the CSU Foundation's budget allocations.

CSU Foundation will be using ArcGIS servers to complete the data storage and mapping tasks associated with the State of Nebraska mapping program. Specifically, CSU Foundation intends to employ the following software applications to complete this task:

- ArcInfo 9.3.1 – highest version of the ArcGIS desktop series with the most functionality. This is needed for high level mapping and analysis.
- ArcEditor 9.3.1 – next level of the ArcGIS desktop series. Less functionality but used for data verification and to ensure data quality.
- ESRI Developer Network – Gives access to scripts and other programming functions that can potentially be used for online mapping applications.
- SQL Server 2005 Enterprise – This is a database used to store spatial and non-spatial data used by ArcInfo, ArcEditor, and ArcGIS server.

CSU Foundation intends to use these software solutions because they are necessary tools to complete the GIS analysis will be performed under this program. These programs integrate seamlessly with other ESRI products. Further, they are integral in performing the necessary verification and error correction functions that are required in the Federal NOFA's technical appendix and required by the State's Request for Proposal.

Figure 7: Broadband Workflow and Network Design



4.5 Detailed Project Work Plan

Section 4.2 outlines a detailed work plan and the functions that Apex and CSU Foundation together will perform to achieve the objectives of this RFP.

4.6 Deliverables and Due Dates

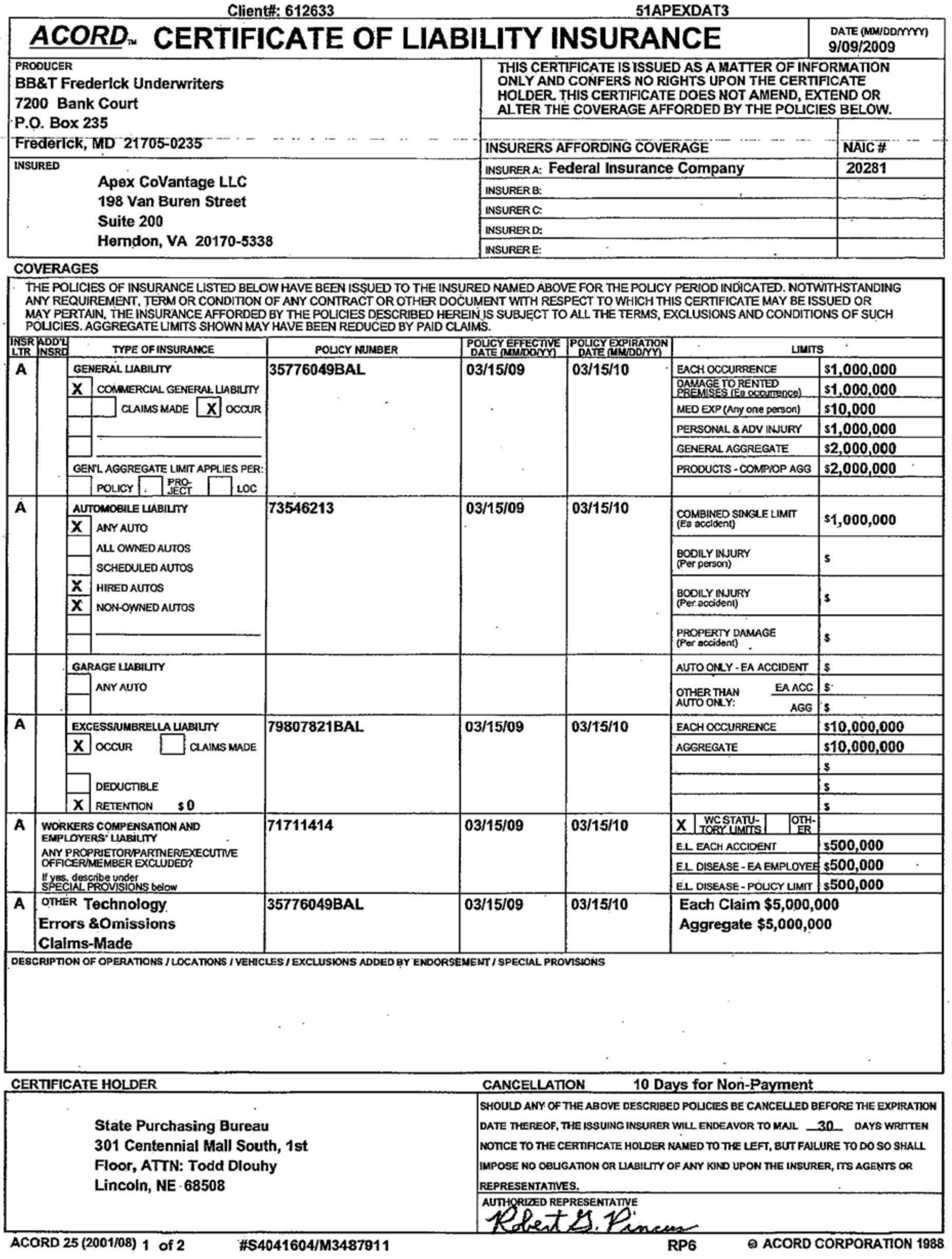
Apex commits to meet the timelines for expedient delivery of data as defined in the NOFA (lines 575-576 and 663- 664), and will be able to deliver a "substantially complete data set" ready to be filed with the NTIA by no later than February 1, 2010. An indicative draft timeline of the activities is presented below.

Table 1: Schedule

	1-Oct-09	1-Nov-09	1-Dec-09	1-Jan-10	1-Feb-10	1-Mar-10
Estimated project start date	▨					
Provider data collection	▨	▨				
Baseline availability assessment	▨	▨				
Database development and ProField customization	▨	▨	▨			
Field Verification and survey		▨	▨	▨	▨	
Preferred: Substantially complete data set submission	▨	▨				
Website Development and Hosting		▨	▨	▨	▨	
Community outreach			▨	▨	▨	▨
Required: Substantially complete data set submission				▨	▨	
Required: Complete GIS-ready data set submission					▨	▨

5.0 Appendix A: Insurance Certificate

On the following page, please find a copy of Apex's insurance certificate, which lists the State of Nebraska as an additional insured, as required.



Client#: 612633 51APEXDAT3

ACORD™ CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 9/09/2009

PRODUCER
BB&T Frederick Underwriters
7200 Bank Court
P.O. Box 235
Frederick, MD 21705-0235

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW.

INSURED
Apex CoVantage LLC
198 Van Buren Street
Suite 200
Herndon, VA 20170-5338

INSURERS AFFORDING COVERAGE	NAIC #
INSURER A: Federal Insurance Company	20281
INSURER B:	
INSURER C:	
INSURER D:	
INSURER E:	

COVERAGES

THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. AGGREGATE LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	ADD'L INSRD	TYPE OF INSURANCE	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YY)	POLICY EXPIRATION DATE (MM/DD/YY)	LIMITS	
A		GENERAL LIABILITY ☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS MADE ☒ OCCUR ☐ ☐ GEN'L AGGREGATE LIMIT APPLIES PER: ☐ POLICY ☐ PRO-JECT ☐ LOC	35776049BAL	03/15/09	03/15/10	EACH OCCURRENCE	$1,000,000
						DAMAGE TO RENTED PREMISES (Ea occurence)	$1,000,000
						MED EXP (Any one person)	$10,000
						PERSONAL & ADV INJURY	$1,000,000
						GENERAL AGGREGATE	$2,000,000
						PRODUCTS - COMP/OP AGG	$2,000,000
A		AUTOMOBILE LIABILITY ☒ ANY AUTO ☐ ALL OWNED AUTOS ☐ SCHEDULED AUTOS ☒ HIRED AUTOS ☒ NON-OWNED AUTOS ☐	73546213	03/15/09	03/15/10	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
						BODILY INJURY (Per person)	$
						BODILY INJURY (Per accident)	$
						PROPERTY DAMAGE (Per accident)	$
		GARAGE LIABILITY ☐ ANY AUTO ☐				AUTO ONLY - EA ACCIDENT	$
						OTHER THAN AUTO ONLY: EA ACC	$
						AGG	$
A		EXCESS/UMBRELLA LIABILITY ☒ OCCUR ☐ CLAIMS MADE ☐ DEDUCTIBLE ☒ RETENTION $0	79807821BAL	03/15/09	03/15/10	EACH OCCURRENCE	$10,000,000
						AGGREGATE	$10,000,000
							$
							$
							$
A		WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? If yes, describe under SPECIAL PROVISIONS below	71711414	03/15/09	03/15/10	☒ WC STATU-TORY LIMITS ☐ OTH-ER	
						E.L. EACH ACCIDENT	$500,000
						E.L. DISEASE - EA EMPLOYEE	$500,000
						E.L. DISEASE - POLICY LIMIT	$500,000
A		OTHER Technology Errors &Omissions Claims-Made	35776049BAL	03/15/09	03/15/10	Each Claim $5,000,000 Aggregate $5,000,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES / EXCLUSIONS ADDED BY ENDORSEMENT / SPECIAL PROVISIONS

CERTIFICATE HOLDER

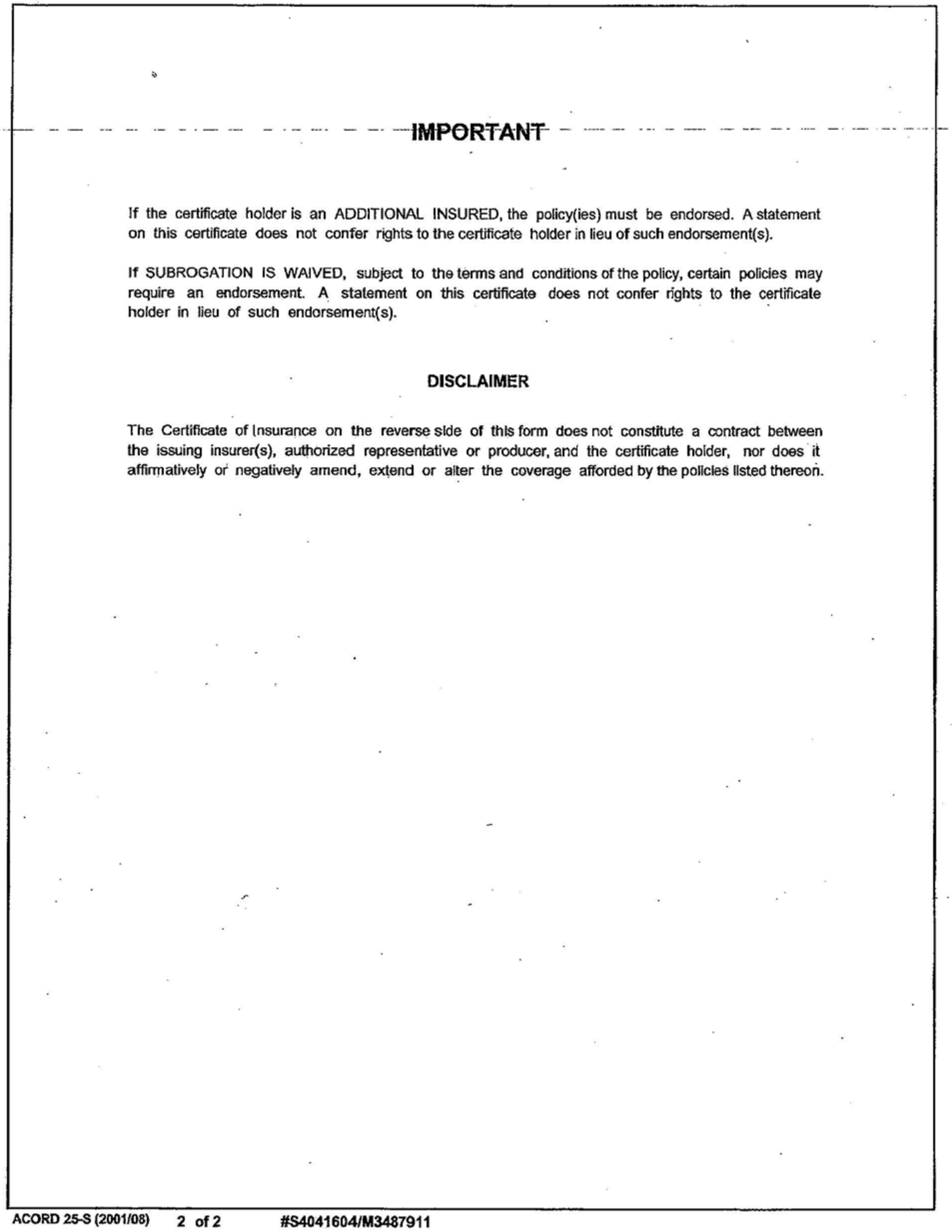
State Purchasing Bureau
301 Centennial Mall South, 1st
Floor, ATTN: Todd Dlouhy
Lincoln, NE 68508

CANCELLATION 10 Days for Non-Payment

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, THE ISSUING INSURER WILL ENDEAVOR TO MAIL 30 DAYS WRITTEN NOTICE TO THE CERTIFICATE HOLDER NAMED TO THE LEFT, BUT FAILURE TO DO SO SHALL IMPOSE NO OBLIGATION OR LIABILITY OF ANY KIND UPON THE INSURER, ITS AGENTS OR REPRESENTATIVES.

AUTHORIZED REPRESENTATIVE
Robert G. Pincus

ACORD 25 (2001/08) 1 of 2 #S4041604/M3487911 RP6 © ACORD CORPORATION 1988



IMPORTANT

If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

DISCLAIMER

The Certificate of Insurance on the reverse side of this form does not constitute a contract between the issuing insurer(s), authorized representative or producer, and the certificate holder, nor does it affirmatively or negatively amend, extend or alter the coverage afforded by the policies listed thereon.

6.0 Appendix B: Sample NDA

On the following page, please find a copy of the non-disclosure agreement that we would use in Nebraska.

NON-DISCLOSURE AGREEMENT

This Non-disclosure Agreement ("Agreement") between Apex CoVantage, LLC, for itself and on behalf of its Affiliates, and ______________________________________, for itself and on behalf of its Affiliates, (the "Parties") is entered into effective this ________ day of ______________, ___ (the "Effective Date"), in connection with the Parties' contemplation of entry into a business relationship. The Parties will be furnishing to each other certain Proprietary Information relating to their businesses and/or products and services, which is non-public, confidential and/or proprietary in nature. The Parties may each be referred to as either the "disclosing party" or the "receiving party" as the context requires. The term "Affiliate(s)" means (a) an entity that owns, directly or indirectly, a majority interest in a Party (a "Parent Company"), or (b) an entity in which a Party or a Party's Parent Company owns, directly or indirectly, a majority interest.

In consideration of each of the Parties furnishing Proprietary Information to the other, the Parties agree as follows:

1. **PROPRIETARY INFORMATION**. As used in this Agreement, "Proprietary Information" means:

   (a) Intellectual property, including trade secrets, copyrights, patents, trademarks and all other proprietary rights, business processes and know-how, methods of business operation, and all documentation pertaining to such information furnished by one party to the other, together with analyses, compilations, studies or other documents prepared by the receiving party or by its agents, representatives (including attorneys, accountants and financial advisors) or employees which contain or otherwise reflect such information.

   (b) Commercial and financial information, including marketing and sales plans, product development plans, competitive analyses, benchmark test results, business and financial budgets, plans or forecasts, non-public financial information, and agreements.

   (c) Software and any documentation or listing pertaining to such software; the term "software" as used in this paragraph refers to software in various stages of development and includes without limitation the literal elements of a program (source code, object code or otherwise), its audiovisual components (menus, screens, structure and organization), any human or machine readable form of the program, and any writing or medium in which the program or the information therein is stored, written or described, including without limitation diagrams, flow charts, designs, drawings, specifications, models, data, bug reports and customer information.

   (d) Information about or relating to any existing, past or prospective customer ("Customer"), or any representative, employee or contractor of Customer ("Customer Representative") including but not limited to (i) all documents or property (a) owned by a Customer, or (b) provided by a Customer directly to the receiving party, or (c) provided by the disclosing party from a Customer to the receiving party (collectively hereinafter "Customer Property"), (ii) Customer names, and names and identifying information of Customer Representative, (iii) organizational charts and information regarding hierarchies, duties, and the like, (iv) Customer preferences, Customer business plans, budgets, and financial information, and (v) lists or databases containing any of the foregoing information (collectively, "Customer Information").

(e) Employee information, including names and addresses and other contact information for past, present and prospective employees, and lists or databases containing such information.

(f) Any information or material not described above which relates to inventions, technological developments, "know how," purchasing, accounting, merchandising, or licensing.

(g) Any information of the type described above which the disclosing party has a legal obligation to treat as privileged or confidential, or which the disclosing party treats as proprietary or designates as privileged or confidential, whether or not owned or developed by the disclosing party.

(h) Any information or material not described above which relates to the disclosing party's commercial and financial activities.

(i) Any information within the scope of Subsections (a) through (h) of this Section 1 exchanged by the Parties before execution of this Agreement and in connection with the project, program or other business opportunity contemplated by the Parties upon execution of this Agreement.

2. **OBLIGATION OF CONFIDENTIALITY.**

(a) The receiving party and its representatives will keep the Proprietary Information provided by the disclosing party strictly confidential and will not, without the prior written consent of the disclosing party: (1) Disclose the Proprietary Information in any manner whatsoever, in whole or in part; (2) Use any of the Proprietary Information, and particularly the Proprietary Information relating to Customers, in any manner that might compete with, interfere with, or harm the other party's business; (3) Reverse engineer, decompile, decipher, disassemble, or decode any Proprietary Information; (4) Attempt to bypass or defeat protections used to prevent unauthorized use of the Proprietary Information; (5) Derive any source code or algorithms of the Proprietary Information by any method whatsoever; or (6) Except as authorized herein make or use, nor allow others to make or use any copies of the Proprietary Information without the disclosing party's prior written consent as to each such copy or use. If such consent is given, all such copies shall be returned to disclosing party when the other party has completed the task for which such copy or use was required.

(b) Each party agrees to use reasonable efforts (meaning efforts not less than those the receiving party employs to protect its own most confidential and proprietary information) to safeguard the Proprietary Information of the other and to prevent its unauthorized, negligent or inadvertent disclosure. None of the Proprietary Information will be used by the receiving party or its representatives other than in connection with the Parties' contemplated project, program or other business opportunity. The receiving party will be responsible for any breach of this Agreement by its representatives, whether they are employees or otherwise.

(c) Notwithstanding the obligations set forth in Subsections 2(a) and 2(b) herein, (i) the receiving party may and is hereby authorized to provide to the National Telecommunications and Information Administration ("NTIA"), U.S. Department of Commerce, all data collected under any State Broadband Data and Development Grant Program authorized by the Broadband Data Improvement Act, and (ii) this Agreement shall not restrict NTIA's use of such data as contemplated by the Notice of Funds Availability, Docket No. 0660-ZA29, dated July 1, 2009, published by NTIA (including sharing such data with the Federal Communications Commission or other federal agencies).

3. **PROJECT NOT TO BE DISCLOSED**. Without the prior written consent of the disclosing party, except and only to the extent required by law, neither the receiving party nor its Representatives will disclose to any person or entity the fact that the Proprietary Information has been made available to it by the disclosing party or any facts regarding the Parties' contemplated project, program or other business opportunity, including its status.

4. **INFORMATION TO BE RETURNED OR DESTROYED**. Except as provided below, the receiving party agrees to promptly return all copies of the Proprietary Information, including any portion of the Proprietary Information that consists of analyses, compilations, forecasts, studies or other documents prepared by the receiving party or its Representatives, to the disclosing party immediately upon its request at any time, or immediately after any decision by either party not to proceed with the contemplated project, program or other business opportunity.

5. **NON-CONFIDENTIAL INFORMATION**. The term Proprietary Information shall not include such information which: (i) is or becomes generally available to the public other than as a result of a disclosure by the receiving party or its Representatives, (ii) becomes available to the receiving party on a non-confidential basis from a source other than the disclosing party which is not prohibited from disclosing such information to the receiving party by a legal, contractual or fiduciary obligation, or (iii) information which is independently developed by the receiving party, as evidenced by written and dated records kept by the receiving party in the ordinary course of business. The receiving party will bear the burden of proof in showing the applicability of one or more of the foregoing exclusions.

6. **LEGALLY COMPELLED DISCLOSURE**. In the event that the receiving party becomes legally compelled to disclose any of the Proprietary Information, the receiving party will provide the disclosing party with prompt notice so that the disclosing party may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement.

7. **DEFINITIVE AGREEMENT**. NEITHER PARTY MAKES ANY WARRANTIES REGARDING THE ACCURACY OF THE PROPRIETARY INFORMATION nor accepts any responsibility for any expenses, losses or action incurred or undertaking by the receiving party as a result of its receiving the Proprietary Information. Unless and until

a definitive agreement has been executed and delivered by the parties, neither party shall be under any legal obligation to undertake any project or any other business relationship.

8. **WAIVER**. It is understood and agreed that no failure or delay in exercising any right, power or privilege hereunder, shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder.

9. **INJUNCTIVE RELIEF, DAMAGES & ATTORNEYS' FEES**. Each party understands that the continued confidentiality of the Proprietary Information is critical to the disclosing party and essential to the continued goodwill and ultimate success and profitability of the disclosing party and that such confidentiality goes to the essence of this Agreement. Accordingly, each party agrees that use or disclosure of the Proprietary Information in a manner inconsistent with this Agreement will cause the disclosing party irreparable damage, that the disclosing party's remedy at law for any actual or threatened breach of this Agreement by the receiving party or its Representatives will be inadequate and that the disclosing party shall be entitled, as a matter of right, to specific performance hereof or injunctive relief, by temporary injunction or other appropriate judicial remedy, writ or order, in addition to any damages that such party may be legally entitled to recover, together with expenses of litigation, including reasonable attorneys' fees incurred in connection therewith.

10. **TERM & TERMINATION**. The term of this Agreement and the receiving party's obligations under this Agreement shall commence on the Effective Date and extend with respect to all Proprietary Information until five (5) years after the date of the last disclosure hereunder. Thereafter, the receiving party's obligations hereunder survive and continue in effect with respect to any Proprietary Information that is a trade secret under applicable law.

11. **SURVIVAL OF AGREEMENT**. The obligations and restrictions set forth in this Agreement regarding the use of the Proprietary Information shall survive termination of this Agreement.

12. **GOVERNING LAW & JURISDICTION**. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, without giving effect to its conflict of laws principles or rules. The parties agree to submit to the jurisdiction and venue of the state and federal courts located in the Commonwealth of Virginia with respect to any dispute arising from this Agreement.

For ______________________________ For ______________________________

Signature: ________________________ Signature: ________________________

Name: ____________________________ Name: ____________________________

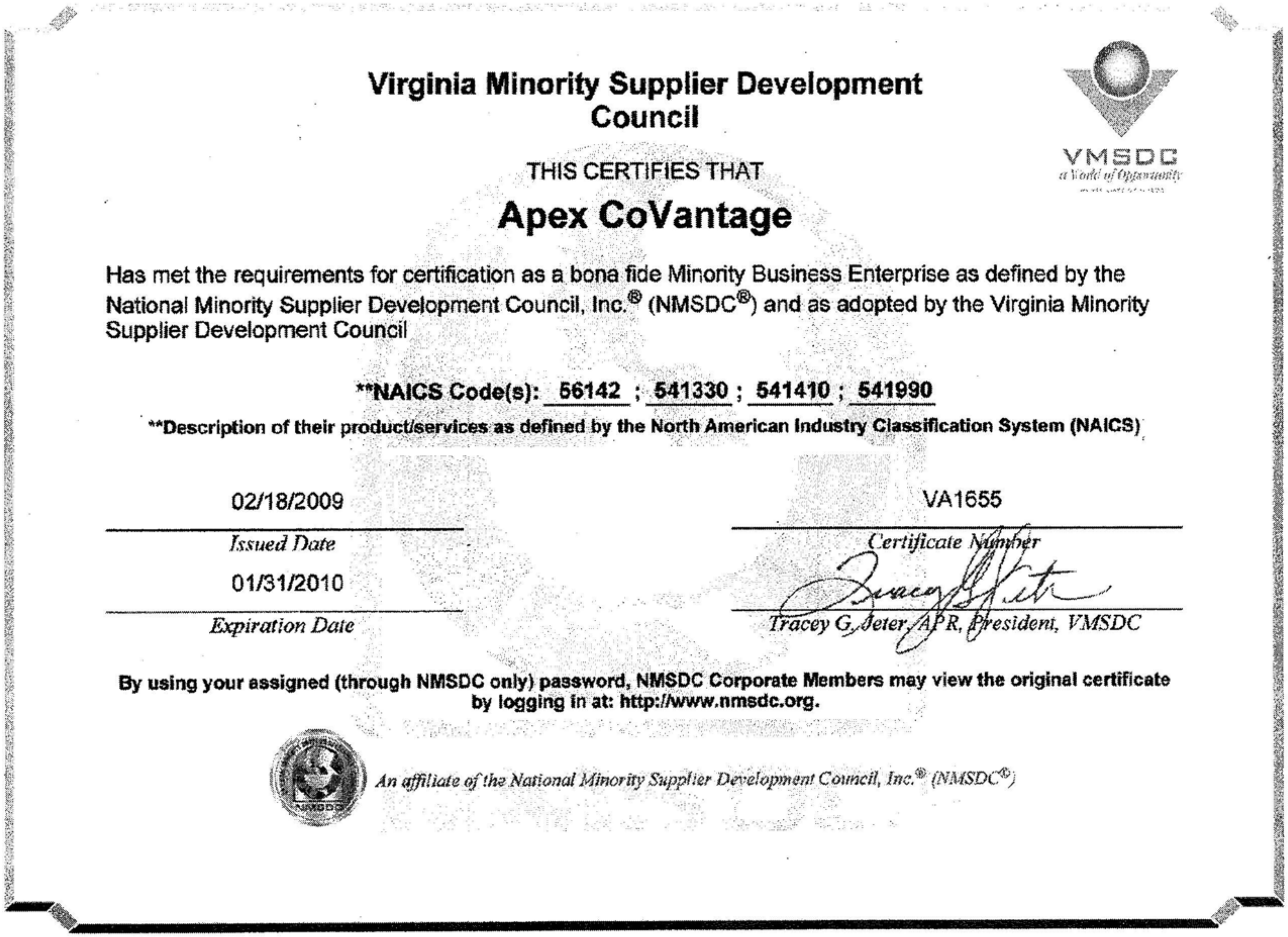
Title: _____________________________ Title: _____________________________

7.0 Appendix C: Minority Certificates

Apex is a minority owned company, certified by a number of state and national organizations. These include:

- Virginia Council of the National Minority Supplier Development Council
- California Public Utilities Commission Supplier Clearinghouse
- Commonwealth of Virginia Department of Minority Business Enterprise

Certificates from these organizations can be found on the following pages.



Virginia Minority Supplier Development Council

VMSDC
a World of Opportunity

THIS CERTIFIES THAT

Apex CoVantage

Has met the requirements for certification as a bona fide Minority Business Enterprise as defined by the National Minority Supplier Development Council, Inc.® (NMSDC®) and as adopted by the Virginia Minority Supplier Development Council

****NAICS Code(s): 56142 ; 541330 ; 541410 ; 541990**

****Description of their product/services as defined by the North American Industry Classification System (NAICS)**

02/18/2009
Issued Date

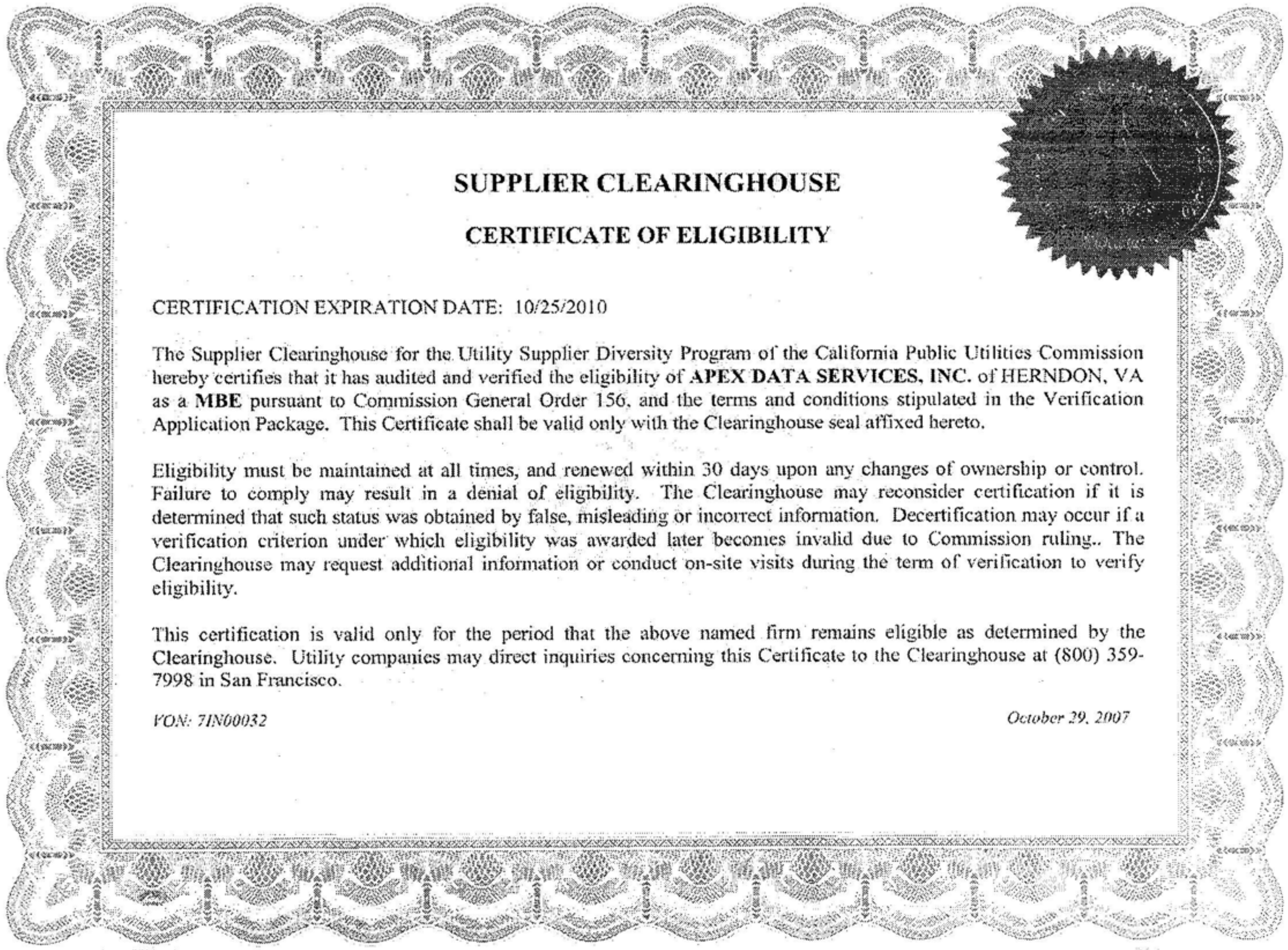
VA1655
Certificate Number

01/31/2010
Expiration Date

Tracey G. Jeter, APR, President, VMSDC

By using your assigned (through NMSDC only) password, NMSDC Corporate Members may view the original certificate by logging in at: http://www.nmsdc.org.

An affiliate of the National Minority Supplier Development Council, Inc.® (NMSDC®)



SUPPLIER CLEARINGHOUSE

CERTIFICATE OF ELIGIBILITY

CERTIFICATION EXPIRATION DATE: 10/25/2010

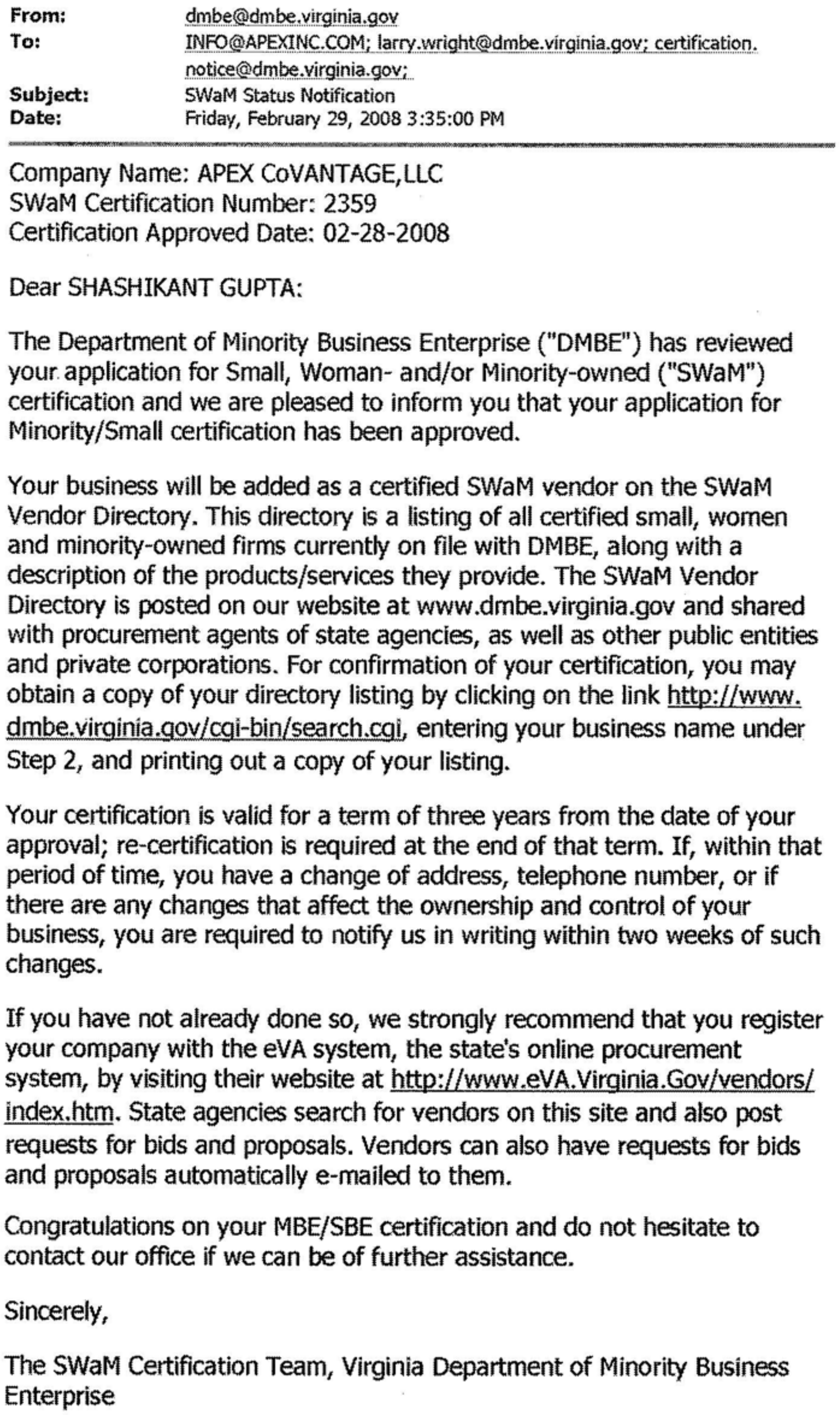
The Supplier Clearinghouse for the Utility Supplier Diversity Program of the California Public Utilities Commission hereby certifies that it has audited and verified the eligibility of **APEX DATA SERVICES, INC.** of HERNDON, VA as a **MBE** pursuant to Commission General Order 156, and the terms and conditions stipulated in the Verification Application Package. This Certificate shall be valid only with the Clearinghouse seal affixed hereto.

Eligibility must be maintained at all times, and renewed within 30 days upon any changes of ownership or control. Failure to comply may result in a denial of eligibility. The Clearinghouse may reconsider certification if it is determined that such status was obtained by false, misleading or incorrect information. Decertification may occur if a verification criterion under which eligibility was awarded later becomes invalid due to Commission ruling.. The Clearinghouse may request additional information or conduct on-site visits during the term of verification to verify eligibility.

This certification is valid only for the period that the above named firm remains eligible as determined by the Clearinghouse. Utility companies may direct inquiries concerning this Certificate to the Clearinghouse at (800) 359-7998 in San Francisco.

VON: 7IN00032

October 29, 2007



From: dmbe@dmbe.virginia.gov
To: INFO@APEXINC.COM; larry.wright@dmbe.virginia.gov; certification.notice@dmbe.virginia.gov;
Subject: SWaM Status Notification
Date: Friday, February 29, 2008 3:35:00 PM

Company Name: APEX CoVANTAGE,LLC
SWaM Certification Number: 2359
Certification Approved Date: 02-28-2008

Dear SHASHIKANT GUPTA:

The Department of Minority Business Enterprise ("DMBE") has reviewed your application for Small, Woman- and/or Minority-owned ("SWaM") certification and we are pleased to inform you that your application for Minority/Small certification has been approved.

Your business will be added as a certified SWaM vendor on the SWaM Vendor Directory. This directory is a listing of all certified small, women and minority-owned firms currently on file with DMBE, along with a description of the products/services they provide. The SWaM Vendor Directory is posted on our website at www.dmbe.virginia.gov and shared with procurement agents of state agencies, as well as other public entities and private corporations. For confirmation of your certification, you may obtain a copy of your directory listing by clicking on the link http://www.dmbe.virginia.gov/cgi-bin/search.cgi, entering your business name under Step 2, and printing out a copy of your listing.

Your certification is valid for a term of three years from the date of your approval; re-certification is required at the end of that term. If, within that period of time, you have a change of address, telephone number, or if there are any changes that affect the ownership and control of your business, you are required to notify us in writing within two weeks of such changes.

If you have not already done so, we strongly recommend that you register your company with the eVA system, the state's online procurement system, by visiting their website at http://www.eVA.Virginia.Gov/vendors/index.htm. State agencies search for vendors on this site and also post requests for bids and proposals. Vendors can also have requests for bids and proposals automatically e-mailed to them.

Congratulations on your MBE/SBE certification and do not hesitate to contact our office if we can be of further assistance.

Sincerely,

The SWaM Certification Team, Virginia Department of Minority Business Enterprise

8.0 Appendix D: Resumes

On the following pages, please find resumes for proposed project staff, as required by Section V Proposal Instructions, A. Technical Proposal, 3 i of the RFP.

Team Member **Anthony Roberts**

Team Role

Executive Project Management

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 709-3452
Email: aroberts@apexcovantage.com

Education and Specialized Training

Mississippi State University, B.S., Industrial Engineering

Experience Summary

Mr. Roberts is the Director of Operations, Engineering Services at Apex. He is responsible for all engineering solutions projects within the company, which range in size from $5 million to $100 million, and he oversees all of the project managers. Mr. Roberts provides fiduciary and quality management of 2,500 personnel in the USA and India. He has experience developing and managing delivery schedules and project specifications unique to each customer, as well as overseeing multiple vendor contracts with broad interaction schemes.

Below is a sampling of projects on which Mr. Roberts has made a significant contribution.

<u>Qwest Posting and Landbase Facilities Conversion</u>: On this OSP-FM conversion project consisting of Work Order posting, landbase creation, and facilities conversion, Mr. Roberts serves as Director of Operations, providing total oversight for all quality, deliverables, and schedule.

<u>AT&T Field Inventory & Mapping</u>: Mr. Roberts was responsible for all quality, escalation processes, delivery schedule, budget, and customer and vendor interaction. He oversaw ten vendors and a staff of over 2,500 resources. The project involved six interdependent work streams, including developing a complex data management software, synthesizing data records across multiple disparate databases, performing a comprehensive field inventory of telecom assets throughout the service territory, migrating engineering data to an updated landbase, posting work orders, and cleansing the facilities

engineering data. The work involved both domestic and international operations, and was managed through a dedicated 20-person Project Integration and Mission Control Office (PIMCO) in Apex's corporate headquarters in Herndon, VA.

AT&T Southeast Construction & Engineering: Responsible for all Construction and Engineering of telephone facilities to enable the corporation to offer video services. Duties included oversight for all hiring, acquisition of vehicles and work space.

AT&T Southeast Network Dispatch Center: Supervised 12 managers responsible for the daily and future load management of POTS, DSL, Special Services, and DLC for the state of Mississippi. Also, responsible for Air Pressure, Testability, and Predictor for the three Gulf States (MS, LA, AL). Managed the MS NDC through the Hurricane Katrina Restoration.

BellSouth Telecommunications, Work Management Center: Supervised eight Load Balance Supervisors responsible for the daily and future load management of the POTS load for Mississippi.

Bellsouth Telecommunications Installation and Repair: Supervised 16 technicians performing installation and maintenance work in 14 wire centers in South MS. Performed quality and safety inspections each month, reviewed and coached technicians for performance improvement, adjusted placement and schedules of technicians to meet load conditions, contacted customers to resolve PSC complaints and customer complaints, handled all TechNet maintenance and downloads, and corrected and reviewed all GPS data.

Hardware/Software Experience	Operating Systems:	MS-DOS, Windows 95, Windows NT, Unix
	Electric Design Software:	GE Smallworld, ESRI ArcMap 8.3, MicroStation V8, AutoCAD 2002/2006, AutoCAD Map 2006
	Other:	Microsoft Office, Microsoft Project, Oracle

Career History	Apex CoVantage, LLC	2008 – Present
	AT&T Southeast	2005 – 2008
	BellSouth Telecommunications	2000 – 2005
	Industrial Engineering Ergonomics Lab	1999

References

Caroline Myers
Qwest
Project Manager
9613 East 146th Ave
Thornton, CO 80602
(720) 540-1015

Rob Ours
AT&T
Area Manager, LA NDC
203 Longpointe Rd
Youngsville, LA 70592
(337) 515-0069

Marc Renkes
Booze Allen Hamilton
Associate
193 Spencer Terrace, SE
Leesburg, VA 20175
(703) 346-9469

Team Member **Bill Jamison**

Team Role

Database and Solutions Architect

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 709-3453
Email: bjamison@apexcovantage.com

Education and Specialized Training

Wright State University, B.S., Management Information Systems

Experience Summary

Mr. Jamison has more than ten years' experience in Information Systems management and design. He has played diverse roles including Software Engineer, Project Manager and Business Developer.

A key strength is Mr. Jamison's ability to add insight and positive direction to on-going system development efforts by identifying inefficiencies, exploring opportunities, and dramatically reducing costs.

Hardware/Software Experience

Database:	SQL Server, Access, Sybase, Oracle
Programming:	VB.Net, C#, JavaScript, HTML, DHTML, ASP.Net
Applications:	MS Project, VStudio, MTS, Modeling Software
Other	Document Management Systems, Enterprise Workflow Systems, Field Workforce Management Systems, GIS

Career History

Apex CoVantage, LLC	2008 – Present
Wysitech, Inc.	2002 – 2008
Access Systems, LLC	2000 – 2002
Reynolds & Reynolds	1997 – 2000

References

Dawn Pate-Cole
AT&T
Alabama Operations Center
Room 107N
3196 Highway 280 South
Birmingham, AL 35243
(205) 969-6968

Mary-Ellen Fremuth
Florida Power and Light
14515 Horseshoe Trace
Wellington, FL 33414
(561) 691-7729

Scott Segalewitz
University of Dayton
9515 Bridlewood Trail
Dayton, Ohio 45458
(937) 229-1036

Team Member **Mr. Aravind Natarajan**

Team Role

Technology Architect

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 709-3454
Email: aravind@apexcovantage.com

Education and Specialized Training

B.S., Computer Engineering, University of Bombay, Bombay, India

M.S., Computer Science, University of Maryland, College Park

Experience Summary

Mr. Natarajan is the Chief Technology Officer of the Technology Products and Solutions Division at Apex. A 16-year veteran of Apex, he is one of its leading technologists and has experience in strategy, planning and new product development with industry skills spanning telecommunications, electric and gas utilities and electronic content solutions. Responsible for many of the innovative technologies developed by Apex over the years, Mr. Natarajan has successfully executed numerous multi-million dollar projects.

He has over a decade of experience in managing complex projects with onshore and offshore components. He has successfully executed numerous multi-million dollar projects within budget and 100% on-time delivery. He has a strong technical background with experience in software development, requirement analysis, and quality control.

Project Experience

Below is a sampling of the projects on which Mr. Natarajan has made a significant contribution.

AT&T: Mr. Natarajan was responsible for working with AT&T to define and document in detail the technical scope of work, quality requirements and procedures for this complex project that involved four different tracks. Mr. Natarajan also managed the entire quality and problem resolution team that formed the core technical team for the AT&T project.

Sacramento Municipal Utility District: As the Technical Project Manager, he was responsible for understanding the source documents, SMUD's distribution network, and the target G/Technology data model. He designed the data conversion process in detail and the software and procedures for loading data into G/Technology. He managed all aspects of the project, including field data collection and conversion and ensured data quality and on-time completion.

American Electric Power: He was involved in the design and development of technical specifications for the CLIF loader for loading data into Smallworld from ASCII files. He designed the export software for exporting data from DataWorks into ASCII files for loading into Smallworld. He was also responsible for ensuring a clean load into AEP's Smallworld database, troubleshooting any import problems and overall quality of the data.

Commonwealth Edison: He designed and customized DataWorks for the project, which included handling complex relationships between ducts, conduits, and cross-sections. He was also involved in the design and development of technical specifications for the CLIF loader for loading data into Smallworld from ASCII files and modeling Internal Worlds and connectivity between external and internal worlds.

Conectiv: As Technical Lead, he customized and developed the DataWorks to CLIF export software, and he supervised the development of the CLIF-to-GE Smallworld application. He designed the process to extract attribute data from Conectiv's Automated Engineering Records (AER) database and link the data to objects captured from the source maps.

Technical Experience

- G/Technology data model expert
- Extensive Smallworld data model experience
- Oracle 8i Certified DBA
- Extensive development of graphic tools using MicroStation MDL, which eases the process of map creation.
- Developed several verification tools to ensure consistency between database and graphics within

DataWorks.

- Developed a table model in C++ that is primarily geared to capture of tabular material from paper documents.
- Enhanced existing coding language to incorporate new features and implemented software that allowed both visual display of tables and translation to SGML, HTML and other proprietary systems.

Software Experience

GIS/AM/FM and CAD Systems:	*Intergraph G/Technology, Bentley MicroStation, GE Smallworld*
Operating Systems:	*MS DOS, Windows 95, Windows NT, Unix*
Languages:	*C++, Perl, MicroStation MDL, GE Smallworld Magik*

Career History

Apex CoVantage, LLC	1992 – present

References

Jim Hayes, Project Manager
Sacramento Municipal Utility District
6301 S Street
Sacramento, CA 95817-1899
(916) 732-6450
JHayes@smud.org

Bill Teager
MidAmerican Energy
2811 5th Ave
Rock Island, Illinois 61201
(309) 793-3625
wfteager@midamerican.com

Sammy Ayyalusamy
President
Wysitech, Inc
5335 Farhills Ave, Suite 211
Dayton, OH 45429
(937) 436-9008 ext 240
sammy@wysitech.com

Team Member	**Mr. Prakash Shinde**

Team Role for this Project

Mapping Manager

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 709-3466
Email: pshinde@apexcovantage.com

Education and Specialized Training

Diploma, Mechanical Engineering, S.J. Polytechnic, Bangalore, India
Graduation Coursework, Computer Application, IGNOU University, New Delhi, India
GE Smallworld User and System Administrator training

Experience Summary

Mr. Shinde is a Project Manager at Apex. Mr. Shinde has a strong background in technical support. His responsibilities have included planning, implementing, scheduling, and training on utility and telecom projects, including managing teams of over 150 personnel and communicating directly with the client on system design, specification, and problem resolution.

Project Experience

Below is a sampling of the projects on which Mr. Shinde has made a significant contribution.

<u>AT&T:</u> Developed Data Management Tool (DMT) requirements, design review and software specification and participated in documenting detailed specification.

<u>Verizon</u>: On this ICGS conversion project, he manages a team of approximately 150 resources and is responsible for project management, schedule and client interaction. The conversion project is done offshore.

<u>ComEd</u>: Provided project planning, implementation, scheduling, and training on project that involved prepping paper sources for conversion into Smallworld.

Conectiv: Provided project planning, implementation, scheduling, and training on project that involved both paper and digital conversion in MicroStation to Smallworld.

American Electric Power: Provided project planning, implementation, scheduling, and training on project that involved adding non-graphic data to existing spatial data without changing the existing network connectivity. Smallworld was the target system.

Baltimore Gas and Electric: Provided project planning, implementation, scheduling, and training on project that involved conversion of paper records into GE Smallworld. Land base was directly converted using a Remote server terminal.

Dominion Power: Provided project planning, implementation, scheduling, and training on work order posting project, which involved connecting to the client's sever to update the work orders and perform QA before posting.

Bell Canada IMAP CableCAD: Managed team of ten digitizers and provided technical support to clarify Bell Canada's record conversion. Also oversaw team of twenty Quality technicians responsible for using visual quality routines and software tools. Visited Montreal to train Data Analysts for duration of pilot project.

Bell Atlantic (BAARS): Scrubbed conduit database, input data, and digitized conduit records, as well as performed quality control. Project involved converting existing plant engineering records, which were maintained in Bell Atlantic Automated Records System, to be displayed into IMAP V3 using Geonet.

Telus (CableCAD to FRAMME): Scrubbed records of copper and fiber cables and digitized paper and digital sources of Beverly/Meadows units. Project involved conversion of 30 telecom wire centers from CableCAD to Intergraph FRAMME.

AD-Dammam Municipality, Saudi Arabia: Performed quality review on pilot project that involved conversion in dxf format.

Technical Experience

- Extensive production and quality management experience
- Involved in training quality and digitizing engineers

Hardware/Software Experience	GIS/AM/FM and CAD Systems:	*AutoCAD, MicroStation, Cadoverlay, CableCAD, IMAP V2.1,GE Smallworld, Intergraph G/Tech, ESRI GIS database, ARES and OptiNT*
	Hardware:	*IBM PCs*
	Operating Systems:	*Windows NT, OS/2WARP, Windows XP*

Career History	Apex CoVantage, LLC	1998 – present
	M/s ICES	1995 – 1998
	2M Company	1990 – 1995

References

Tim Dummitt

[redacted]

Jason Bruckner

[redacted]

Amar Melige

[redacted]

Team Member **Mr. Ratheesh Nair**

Team Role for this Project

Systems Integration/Database Design

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 709-3449
Email: ratheesh@apexcovantage.com

Education and Specialized Training

Post Graduate Diploma in Computer Application from OACT, India

Experience Summary

Mr. Ratheesh Nair is a software engineer with Apex. He has more than eight years experience in designing and developing software and database systems. He has strong background in C/C++, PL/SQL and database design. He has customized Apex's ProField for different projects targeting diverse platforms, according to the client's specifications.

Project Experience

Below is a sampling of the projects on which Mr. Nair has made a significant contribution:

<u>Verizon</u>: Performed installation of IDDS software and administered Oracle database on HP Unix server. Provided Oracle DBA and delivery support to the IDDS conversion project team.

<u>Sacramento Municipal Utility District</u>: Developed DataWorks, ODAPI, and export software using Oracle PL/SQL and C++.

<u>Baltimore Gas and Electric</u>: Participated in both gas and electric conversion projects. He developed applications to extract data from customer's legacy applications and integrate it with DataWorks data.

<u>Wayne County</u>: Customized DataWorks software and ODAPI software using Oracle PL/SQL and C++. He developed applications to convert DataWorks data to the target database.

Commonwealth Edison: Developed DataWorks software using PL/SQL and C++ to support this electric conversion project.

Bell Canada: Developed applications to capture data from the source using Oracle and C++.

Technical Experience

- Extensive programming experience in C/C++ and Oracle PL/SQL.
- Designed and developed applications to capture data from source.
- Developed ProACT®, Apex's proprietary ERP solution.
- Developed IZAAC® (Intelligent Zoning And Algorithmic Conversion) Apex's proprietary image based text conversion system.

Hardware/Software Experience

Hardware:	*IBM PC, IBM ES 9000, HP K9000*
Operating Systems:	*Windows, Linux, MVS*
Database:	*Oracle, Microsoft SQL Server*
Languages:	*C/C++, C#.NET, VB, PL/SQL*

Career History

Apex CoVantage	1999 – present
International Comptech Engineering Services	1997 – 1999
HighTech Services	1995 – 1997

References

Pardha Karamshetty
Columbia Books INC,
8120 Woodmond Ave, Suite 110
Bethesda, MD 20814
(703) 731 6147

Hu Yu
[redacted]

Venkat Movva
[redacted]

Team Member **Shane Harrison**

Team Role

Project Manager

Contact Information

Apex CoVantage
198 Van Buren Street, Ste. 200
Herndon, VA 20170

Phone: (703) 389-5528
Email: sharrison@apexcovantage.com

Education and Specialized Training

Mississippi State University, Bachelor, Landscape Architecture
Hinds Community College, Associate, Liberal Arts

BellSouth MSOC Certification (Management System and Operating Control)

Experience Summary

Mr. Harrison is a Project Manager at Apex. He has eight years of experience in the geospatial engineering arena, with more than half of that spent in management positions. His experience includes managing large teams of company and vendor personnel, allocating work packages to maintain adherence to aggressive schedules, and developing training schedules and safety programs.

Mr. Harrison is the primary client liaison for all project matters on a day-to-day basis, whether the issue is commercial, technical or schedule in nature.

Below is a sampling of projects on which Mr. Harrison has made a significant contribution.

Qwest Posting and Landbase Facilities Conversion: On this OSP-FM conversion project consisting of Work Order posting, landbase creation, and facilities conversion, Mr. Harrison is responsible for managing the day-to-day operations, production facilities, schedule adherence, and quality.

AT&T Work Order Posting: On this Outside Plant field records conversion and maintenance project, Mr. Harrison was responsible for managing the day-to-day operations, production facilities, vendor schedule adherence, and quality. The project entailed performing work order posting to over 40,000 engineering work orders, with a total of 164,000 work prints completed within a tight timeframe. Project quality exceeded 98%, which was greater than the industry standard of 95%. The success of this project was instrumental in AT&T increasing allocation of work to Apex.

AT&T Field Inventory: This physical inventory project encompassed visiting 75,000 remote terminals across 13 states, which required 578 field auditors and six subcontracted companies. Mr. Harrison was responsible for allocating work to vendors and schedule adherence, ensuring that the aggressive schedule was met. The project was completed within schedule and budget. Project entailed recording predefined attribute information and GPS locations, as well as capturing field conditions via digital photography, which would then allow AT&T's engineers to "desktop engineer" new work orders from across the country without having to visit the sites.

BellSouth Central Office Records Maintenance Project: Mr. Harrison served several roles during his tenure on this Telco central office drafting operations project. As a production supervisor, he managed a team of 25 drafters; developed and maintained production process to meet schedule, performance, and quality targets; and served as the client liaison. He also held the position of Team Lead, in which he was responsible for 15 drafters and developed methods and standards to streamline productivity. He also worked as a GIS Technician and Quality Assurance Technician.

BellSouth/AT&T Telecommunications**:** Mr. Harrison was responsible for supervising 12 dispatch assistants and served as the point of contact for various departments including SSI&M, DLC, BRC, ACAC and others. He created developmental plans to further increase the knowledge and abilities of direct reports through various training, and overall improvement courses; scheduled work duties daily based on the anticipated work load from historical data; and conducted safety observations.

BellSouth Telecommunications: Mr. Harrison served as First Line Network Manager for South Mississippi Turf Installation and Maintenance; was responsible for compiling and reporting multiple documents to help support and develop other Network Managers and

Technicians throughout the turf. He was responsible for developing training programs and facilitating training of Technicians and Supervisors in new tools.

Software Experience	Operating Systems:	Windows NT and XP
	Electric Design Software:	MicroStation, BSTCAD, AutoCAD 14 through AutoCAD 2008, Arc View GIS, MTAS/DB2, IDS, WFA-C
	Other Software:	MS Project, MS Office

Career History	Apex CoVantage, LLC	2008 – Present
	BellSouth	2005 – 2008
	QC Data, Inc.	2001 - 2005

References

Angela O'neal
AT&T
Area Manager
410 Meadowbrook Dr
Jackson, MS 39206
(601) 321-3100

John Audley
AT&T
C&E OSS Manager
7400 Johnson Dr., 1st Floor
Overland Park, KS 66202
(913) 676-0750

Cheryl Fallos
Qwest
Manager Process Management
700 W Mineral Ave, SD-D19.12
Littleton, CO 80120
(303) 707-7361

Dr. Robert Loube

Contact
Office: (240) 393-0259
[redacted]

Education
Ph.D., Economics, Michigan State University, 1983
M.A., Economics, University of Massachusetts-Amherst, 1971
B.S., Economics, University of Maryland-College Park, 1969

Regulatory Experience

Vice President
Rolka Loube and Saltzer Associates
April 2007 to Present

Selected Testimony:

- Filed an expert report on behalf of the U.S. Department of Justice, the United States District Court for the Western District of Texas, San Antonio Division, AT&T Inc, Plaintiff, v. United States of America, Defendant, Civil No. SA-07-CA-0197-OG, October 14, 2008.
- Testified on behalf of the Maine Office of the Public Advocate in the Joint Application for Approvals Related to Verizon's Transfer of Property and Customer Relations to Company to be Merged with and into Fairpoint Communications, Inc. Maine Public Utilities Commission Docket No. 2007-67 on October 2, 2007.

Director, Economic Research
Rhoads & Sinon, LLC
April 2001 to March 2007

Selected Testimony:

- Testified on behalf of the Washington Public Counsel in the Matter of the Petition of Qwest Corporation to be Regulated Under An Alternative Form of Regulation, WUTC Docket No. UT-061625, March 14, 2007.
- Testified on behalf of the Maine Office of Public Advocate in the Investigation Into Verizon Maine's Alternative Form of Regulation, Phase I, Docket No. 2005-155, October 17 and October 18, 2006.
- Filed a declaration on behalf of The Utility Reform Network in re: Investigation on the Commission's Own Motion into Open Access and Network Architecture Development of Dominant Carrier Networks, Verizon UNE Phase, Investigation 93-04-002, filed August 6, 2004

Industry Economist, GS 301-15
Federal Communications Commission
May 1996 to April 2001

Responsibilities include:

- Established the criteria for choosing the universal service economic cost model;
- Evaluated and modified telephone cost models;
- Conducted special studies for use by the Chairman, Commissioners, Bureau Chief or Division Chief

Director, Office of Economics
Public Service Commission of the District of Columbia,
February 1993 to May 1996

Responsibilities include:

- Supervised the preparation of staff testimony in telephone, electric and gas utility cases.
- Prepared and presented testimony on the strategic approach to electricity demand side management and least cost planning principles.

Senior Telecommunications Economist
Public Service Commission of the District of Columbia, May 1989 to the February 1993

Responsibilities include:

- Prepared and presented testimony regarding telephone rate structure, competition in telephone markets, embedded cost studies, and long run incremental cost studies.
- Represented the Commission on digital deployment and generic cost manual working groups.

Econometrician,
Indiana Utility Regulatory Commission,
March 1988 to May 1989

Responsibilities include:

- Developed electric energy and demand forecasts.
- Supervised consultants developing economic and demographic models for utility service territories.

Principal Utility Analyst,
Indiana Utility Regulatory Commission,
January 1986 to March 1988

Responsibilities include:

- Prepared and presented testimony regarding demand and financial forecasting for telephone and electric services, cost of equity and long run marginal cost.
- Contributed to staff reports on energy and demand forecasts.

Selected Publications

"The Telecommunications Act of 1996: Residential Rates and Competition," *Utilities Policy*, September 2004.

"Public Interest Regulation, Common Costs and Universal Service," eds. Edythe S. Miller and Warren J. Samuels, *An Institutionalist Approach* to Public Utilities Regulation, Michigan State University Press, 2002.
"Measuring the Total Service Long-Run Incremental Cost," *Ninth NARUC Biennial Regulatory Information Conference*, September 1994 (with David Gabel and Mark Kennet).
"The Institutional Conditions for Technological Change: Fiber to the Home," *Journal of Economic Issues*, Vol. XXV, No. 4, December 1991.

Selected Staff Testimony

Before the Public Service Commission of the District of Columbia:

Formal Case No. 929 The Application of Potomac Electric Power Company for an Increase in its Retail Rates for the Sale of Electric Energy.

Formal Case No. 850 Investigation into the Reasonableness of the Authorized Return on Equity, Rate of Return, and Current Charges and Rates for Telecommunications Services Offered by the Chesapeake and Potomac Telephone Company

Before the Indiana Utility Regulatory Commission:

Cause No. 38426 Petition of GTE-Indiana
Principal Issues: Revenue Adjustment, Cross-Subsidization, Cost Methodology and Demand Repression

Cause No. 38045 Petition of Northern Indiana Public Service Company
Principal Issues: Demand Forecasting, Financial Viability and Regulatory Policy with Regard to Excess Capacity

References

William Black
Assistant Public Advocate
Maine Office of the Public Advocate
112 State House Station
Augusta, ME 04333
William.C.Black@Maine.Gov
(207) 287-2445

Mr. Joel H. Cheskis
Assistant Consumer Advocate
Pennsylvania Ofc of Consumer Advocate
555 Walnut Street, 5th Floor, Forum Place
Harrisburg, PA 17101-1923
jcheskis@paoca.org
(717) 783-5048

Gary L. Field
Field Law Group, PLLC
915 N. Washington Avenue
Lansing, MI 48906
glfield@fieldlawgroup.com
(517) 913-5100

CATHY EMERSON
Project Manager
Center for Economic Development
35 Main Street
California State University
Chico, CA 95929-0327
530.898.3862
cmemerson@csuchico.edu

EDUCATION

- Master of Science, Organization Development, Applied Behavioral Sciences; School of Public, Affairs, American University/National Training Labs, Washington, D.C. (Graduation: Dec'09)
- Bachelor of Arts, English, Goucher College, Baltimore, MD.

CERTIFICATIONS

- Trainer/Certified Administrator, Myers-Briggs Type Indicator (MBTI©).

EMPLOYMENT

- Project Manager, Broadband, Center for Economic Development, CSU-Chico, CA (2009)
- Organization Development Practitioner/Instructor/Trainer, Roseville, CA (2002-2009)
- Project Manager/Contractor, Volt Information Services, Inc., Cupertino, CA (2001)
- Tenant Coordinator, Parsons Infrastructure & Technology (SFO Associates), San Francisco International Airport, San Francisco, CA (1999-2001)
- Operations & Construction Manager, Ronald Reagan National Airport, Arlington, VA (1989-1996)

Cathy currently manages two broadband demand and supply aggregation projects in counties located in northern California. Since May, she has facilitated more than a dozen structured meetings and workshops to acquire information from both the end-users and suppliers of broadband. She has facilitated acquisition of maps and shape files of current coverage areas from Internet Service Providers. In her capacity as Project Manager, she has overall responsibility for coordinating both the survey research data collection on the use and speed of high speed Internet services and the public release of both survey and coverage mapping results via a public web site.

During her tenures at both San Francisco's International Airport (SFO) and Ronald Reagan National Airport (DCA), she coordinated over 100 different entities through the design, development and construction of new facilities, significant portions of which included the coordination of multiple teams from different arenas dedicated to the design and implementation of new fiber-optic cabling. At SFO, she coordinated the design & construction process for 94 tenants (airlines, all retail, food & beverage operators, and non-revenue passenger services).

REFERENCES

Gladys Palpallatoc
Associate Vice President
California Emerging Technology Fund
The Hearst Building
5 Third Street, Suite 520
San Francisco, CA 94103
(415) 744-2387
Gladys.palpallatoc@cetfund.org

Ofer Tenenbaum
Owner, Valley Internet/PNC
75 Oak Springs Drive
Napa, CA 94558
(707) 422-1200
ofer@pnc.net

Andrew Cardin
Vice President, DigitalPath, Inc.
275 Airpark Boulevard, Suite 500
Chico, CA 95973
530-571-7541
acardin@digitalpath.net

JAMES FLETCHER, PhD

Director, Program for Applied Research and Evaluation (PARE)
35 Main Street
California State University
Chico, CA 95929-0327
530. 898.4332
jfletcher@csuchico.edu

EDUCATION

- BS, Texas A&M University, 1973
- MS, Texas Tech University, 1976
- Ph. D., Michigan State University, 1978

EMPLOYMENT

- Director, Survey Research Center, CSU, Chico, 1994
- Director, Applied Research and Evaluation, CSU, Chico, 2002

EXPERIENCE

Dr. Fletcher's duties have included development of qualitative and quantitative research plans, sampling schemes, questionnaire development, focus group development and management, data collection, data analysis, and report preparation for private for profit businesses, non-profit organizations, and local, state and federal government agencies. His areas of expertise include survey research methods for telephone, mail, Internet, and in-person survey including survey development, sample design and control for non-response bias, and data analysis and reporting. During his 32 year career, Dr. Fletcher has completed more than 100 survey research projects that range from local to national in scope.

Since 2008, Dr. Fletcher has managed three separate Broadband Demand and Supply Aggregation Surveys in separate project areas in Northern California. Together, these studies captured data on the demand for and supply of high speed Internet access and services across sixteen counties, comprising over 1.275 million people, and over 37,400 square miles.

REFERENCES

Michael Morris
California Public Utility Commission
505 Van Ness Avenue, 3rd Floor
San Francisco, CA 94102-3298
(415) 703-2112
mmo@cpuc.ca.gov

Jerry Kashiwada
California Department of Fish and Game
19160 South Harbor Drive
Fort Bragg, CA 95437
(707) 964-5791
jkashiwada@dfg.ca.gov

Brent Smith
Sierra Economic Development Corporation
500 Wall Street, Suite F
Auburn, CA 95603
(530) 823-4703
Brent@seddcorp.biz

ERIK FINTEL
GIS Senior Analyst
Geographical Information Center (GIC)
35 Main Street
California State University, Chico, CA 95929-0327
530.898.3850
efintel@gic.csuchico.edu

EDUCATION

- Bachelor of Arts, 2001. California State University, Chico. Major in Geography and Planning (GIS and Environmental Geography focus).

RELEVANT TRAINING

- Exploring the VBA Environment, ESRI
- Introduction to ArcLogistics, ESRI
- Learning ArcIMS, ESRI
- Working with ArcPad 7, ESRI
- What's new in ArcGIS Server at 9.2, ESRI
- Building Applications with ArcGIS Server Using the Microsoft .NET Framework, ESRI

EMPLOYMENT

- GIS Senior Analyst, Geographical Information Center. (2009)
- GIS Analyst, Geographical Information Center. (2001)
- GIS Assistant, Geographical Information Center. (2000)
- GIC Intern. Geographical Information Center. (2000)

EXPERIENCE

Erik Fintel is responsible for assisting the Project Manager on all research and development, project planning, and methodology implementation. He also supervises all internships and GIS Assistants. He has been an analyst for 8 years and was just recently promoted to Senior Analyst. He has developed and maintained parcel base mapping and street level geocoding models for many organizations, including E911 systems. He has extensive experience with database management systems and Geodatabase management and design. Erik is part of the GIS team that has been working directly with the California Public Utilities Commission GIS staff to assist with conversion tools and aggregation processes, which included a dynamic coding interface, for updating the California Broadband Task Force Existing Broadband Mapping. For the past 18 months, Erik has been assisting the GIS team building the data side of a web based mapping application for California Emerging Technology Fund Aggregate Demand projects. He runs the wire line decay and RF penetration models. Erik assists in the support many California Internet Service Providers collecting accurate data for recent ARRA funding applications and building strong relationships with them to map their existing and proposed service areas by speed, equipment, and provider.

REFERENCES

Darren Sandford
Vice President, Technology Deployment
California Emerging Technology Fund
The Hearst Building
5 Third Street, Suite 520
San Francisco, CA 94103
(415) 744-2389
DSandford@cetfund.org

Tito Vandermeyden
Research Program Specialist (GIS),
California Public Utility Commission
505 Van Ness Avenue, 3rd Floor
San Francisco, CA 94102-3298
(415) 703-5468
tvm@cpuc.ca.gov

Jason Schwenkler
Interim Director,
Geographical Information Center
CSU, Chico 95929
(530) 680-3653
schwenkl@gic.csuchico.edu

	Accessibility Policy
	Accessibility Architecture
	October 31, 2001
	August 22, 2001

A. *Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

B. *Purpose and Objectives*

The purpose of this document is to define and clarify policies, standards, and guidelines that will help agencies meet the needs of people with disabilities.

Neb. Rev. Stat. §73-205 required the Commission for the Blind and Visually Impaired, the Nebraska Information Technology Commission, and the Chief Information Officer to develop a technology access clause by January 1, 2001. The Technology Access Clause applies to all purchases of information technology. The clause includes the following provisions:

> "The intent and purpose of these standards is to ensure that the needs of Nebraskans with disabilities are met through reasonable accommodation of the information technology products and services of the state. Future information technology products, systems, and services including data, voice, and video technologies, as well as information dissemination methods, will comply with the following standards to the greatest degree possible.
>
> 1. Effective, interactive control and use of the technology including, but not limited to, the operating system, applications programs, and format of the data presented must be readily achievable by individuals with disabilities. The intent is to make sure that all newly procured information technology equipment; software and services can be upgraded, replaced or augmented to accommodate individuals with disabilities.
> 2. Information technology made accessible for individuals with disabilities must be compatible with technology used by other individuals with whom the individual with a disability must interact.
> 3. Information technology made accessible for individuals with disabilities must be able to be integrated into networks used to share communications among employees, program participants, and the public.
> 4. Information technology made accessible for individuals with disabilities must have the capability of providing equivalent access to telecommunications or other interconnected network services used by the general population.
> 5. These provisions do not prohibit the purchase or use of an information technology product that does not meet these standards provided that:
>   a. There is no available means by which the product can be made accessible and there is no alternate product that is or can be made accessible; or
>
>   b. The information manipulated or presented by the product is inherently unalterable in nature (i.e., its meaning cannot be preserved if it is conveyed in an alternative manner).

c. The information technology products or services are used in conjunction with an existing information technology system, and modifying the existing system to become accessible would create an undue burden.

d. The agency is able to modify or replace the information technology product with one that will accommodate the needs of individuals with disabilities.

"When development, procurement, maintenance, or use of electronic and information technology does not meet these standards, individuals with disabilities will be provided with the information and data involved by an alternative means of access."

The primary objectives of accessibility standards and guidelines include:

1. Where feasible, people with disabilities can use the same information technology systems as people without disabilities;
2. Early planning for accessibility will make it easier to provide reasonable accommodations when information technology systems are not accessible.

C. Standards and Guidelines

1. FUNCTIONAL PERFORMANCE CRITERIA (SECTION 1194.31)
   a. General-Alternative Access
      (1) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.
      (2) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.
      (3) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided.
      (4) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.
      (5) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.
      (6) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.

2. SOFTWARE APPLICATIONS AND OPERATING SYSTEMS (SECTION 1194.21)
   a. Navigation

(1) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.

(2) A well defined, on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.

b. Image / Information Display

(1) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text.

(2) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.

(3) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.

(4) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.

c. Compatibility.

(1) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.

d. Use of Color

(1) Applications shall not override user selected contrast and color selections and other individual display attributes.

(2) Color-coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(3) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.

e. Animation

(1) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.

f. Forms.

(1) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

3. WEB-BASED INTERNET INFORMATION AND APPLICATIONS (SECTION 1194.22)
   a. Navigation
      (1) Redundant text links shall be provided for each active region of a server-side image map.
      (2) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.
      (3) Row and column headers shall be identified for data tables.
      (4) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.
      (5) Frames shall be titled with text that facilitates frame identification and navigation.
      (6) A method shall be provided that permits users to skip repetitive navigation links.
   b. Image / Information Display
      (1) Documents shall be organized so they are readable without requiring an associated style sheet.
      (2) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.
      (3) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.
      (4) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.
      (5) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with the provisions of Section 2 (Software Applications and Operating Systems), above.
   c. Information Display Alternatives
      (1) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).
      (2) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.
      (3) Use of Color
         (a) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.
      (4) Forms
         (a) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.
      (5) Timed Responses.
         (a) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

4. TELECOMMUNICATIONS PRODUCTS (SECTION 1194.23)
   a. Image / Information Display
      (1) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.
      (2) Products that transmit or conduct information or communication shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.
   b. Technology Links Compatibility
      (1) Telecommunications products or systems, which offer voice communication but do not include TTY functionality, shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.
      (2) Telecommunications products, which include voice communication functionality, shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.
      (3) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.
      (4) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.
   c. Volume Control
      (1) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.
      (2) If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use.
   d. Voice Mail
      (1) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.
      (2) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.
   e. Controls or Keys / Physical Operation

(1) Products, which have mechanically operated controls or keys, shall comply with the following: Controls and Keys shall be tactilely discernible without activating the controls or keys.
(2) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be operable with one hand and shall not require tight grasping, pinching, twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2N) maximum.
(3) Products, which have mechanically operated controls or keys, shall comply with the following: If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.
(4) Products which have mechanically operated controls or keys shall comply with the following: The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.

5. VIDEO AND MULTI-MEDIA PRODUCTS (SECTION 1194.24)
   a. TV
      (1) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, wide screen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.
      (2) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.
   b. Video & Multi-Media
      (1) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned.
      (2) All training and informational video and multimedia productions, which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.
      (3) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.

6. SELF-CONTAINED, CLOSED PRODUCTS (SECTION 1194.25)
   a. Self-contained products shall be usable by people with disabilities without requiring an end-user to attach Assistive Technology to the product. Personal headsets for private listening are not Assistive Technology.
   b. Response Time

(1) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

c. Controls or Keys / Physical Operation

(1) Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with the provisions in Section 4.e, above.

(2) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

d. Audio / Voice Output

(1) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at anytime.

(2) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.

(3) Use of Color

(a) Color-coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(b) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.

(4) Image / Information Display

(a) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(5) Location Accessibility

(a) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length on products which are freestanding, non-portable, and intended to be used in one location and which have operable controls.

(b) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.

(c) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.

(d) Products, which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Operable controls shall not be more than 24 inches behind the reference plane.

7. DESKTOP AND PORTABLE COMPUTERS (SECTION 1194.26)
   a. Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.
   b. Controls or Keys / Physical Operation
      (1) All mechanically operated controls and keys shall comply with the provisions of Section 4.3, above.
      (2) If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with the provisions of section 4.3, above.
   c. When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

D. Key Definitions

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Alternate formats are usable by people with disabilities and may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with this part.
3. Alternate methods are different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.
4. Assistive technology includes any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.
5. Electronic and information technology includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones) information kiosks, and transaction machines, World Wide Web sites, multimedia, and office equipment such as copies and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where

information technology is integral to its operation, are not information technology.

6. Equivalent facilitation provides that nothing in this part is intended to prevent the use of designs or technologies as alternatives to those prescribed in this part provided they result in substantially equivalent or greater access to and use of a product for people with disabilities.
7. Information technology is any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
8. Operable controls are the component of a product that requires physical contact for normal operation. Operable controls include, but are not limited to, mechanically operated controls, input and output trays, card slots, keyboards, or keypads.
9. Product is an electronic and information technology.
10. Self-contained, Closed Products are products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar types of products.
11. Telecommunications are the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.
12. TTY is an abbreviation for teletypewriter. Machinery or equipment that employs interactive text based communications through the transmission of coded signals across the telephone network. TTY's may include, for example, devices known as TDDs (telecommunication display devices) or telecommunication devices for deaf persons) or computers with special modems. TTYs are also called text telephones.
13. Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an agency shall consider all agency resources available to the program or component for which the product is being developed, procured, maintained, or used.

E. Applicability

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these accessibility policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

COMPLIANCE AND ENFORCEMENT STATEMENT

The Governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information accessibility efforts. Such policies should be reasonable and effective. The NITC intends to incorporate adherence to accessibility policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for accessibility improvements during the budget process.

F. *Responsibility*

An effective program for accessibility involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate accessibility for information systems through adoption of policies, standards, and guidelines.
2. Technical Panel Accessibility Work Group. The NITC Technical Panel, with advice from the Accessibility Work Group, has responsibility for recommending accessibility policies and guidelines and making available best practices to operational entities.
3. Assistive Technology Partnership. The Nebraska Assistive Technology Partnership provides training, loan devices and support for accommodations in compliance with Section 508 and the Technology Access Clause. Training and support is available to governmental agencies, schools, businesses, and non-profit organizations.
4. University of Nebraska Accommodation Resource Center. The Accommodation Resource Center (ARC) provides training, loan devices and support for accommodation using assistive technology in both the education and employment environment. The ARC website is http://ar.unl.edu
5. Federal Information Technology Accessibility Initiative. The Federal Information Technology Accessibility Initiative (FITA) is an interagency effort, coordinated by the General Services Administration, to offer technical assistance and to provide an information means of cooperation and sharing of information on implementation of Section 508. Questions about 508 standards can be sent to 508@access-board.gov .
6. Web Accessibility Initiative The Web Accessibility Initiative has created guidelines, which are grouped by priority and are very similar to the final Section 508 rules. The guidelines can be found at http://www.w3.org/wai .
7. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for accessibility of information resources that are consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
8. Information Technology Staff. Technical staff must be aware of the opportunities and responsibility to meet the goals of accessibility of information systems.

G. *Related Policies, Standards and Guidelines*

1. Nebraska Technology Access Clause
2. Nebraska Technology Access Clause Checklist (Questions to Consider)
    a. Desktop and Portable Computers
    b. Video and Multimedia Products
    c. Software Application and Operating Systems
    d. Self-Contained, Closed Products
    e. Telecommunications Products
    f. Web Page Accessibility Questionaire
3. Section 504 of the Rehabilitation Act
4. Electronic and Information Technology Accessibility Standards, Architectural and Transportation Barriers Compliance Board, 36 CFR Part 1194 can be found at http://www.access-board.gov/sec508/508standards.htm

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Geospatial Metadata Standard

Category	**Data and Information Architecture**
Title	**Geospatial Metadata Standard**
Number	

Applicability

☑ **State Government Agencies**
☑ All.. **Standard**
□ Excluding _______________......**Not Applicable**
☑ **State Funded Entities -** All entities receiving state funding for matters covered by this document.......................... **Standard**
☑ **Other: Public Entities-** Other public entities developing or acquiring geospatial data not supported by state funding ....**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of NITC Technical Panel.
Guideline - Adherence is voluntary.

Status: ☑ Adopted □ Draft □ Other:________

Dates:
Date: September 13, 2005
Date Adopted by NITC: September 23, 2005
Other:

Prepared by: Nebraska GIS Steering Committee for consideration by Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-572(2c), 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

All state agencies and entities that receive state funding used, directly or indirectly, for geospatial data development or maintenance shall ensure that geospatial data it collects, produces, maintains, or purchases and which is used for policy development, implementation, or compliance review is documented with metadata compliant with the latest version of the Federal Geographic Data Committee (FGDC) Content Standards for Digital Geospatial Metadata.

1.1 Steps/Timeline for Implementation

a. State agencies and other applicable state funded entities shall institute procedures for complying with standard for new geospatial data development or acquisition upon adoption of standard by the NITC.

b. State agencies shall complete initial listing of existing, applicable geospatial data holdings within three months of the adoption of standard by NITC.

c. State agencies shall complete meta-lite documentation of existing, applicable geospatial data holdings within six months of the adoption of standard by NITC.

d. State agencies shall complete FGDC-compliant metadata documentation of existing and applicable geospatial data holdings within 12 months of the adoption of standard by NITC.

2.0 Purpose and Objectives

The purposes of this standard is to preserve the public's investment in geospatial data, to save public resources by avoiding unnecessary duplication of expensive geospatial data acquisition, to minimize errors through inappropriate application of geospatial data, and to facilitate harmonious trans-agency public policy decision-making and implementation through the use of shared geospatial data.

2.1 Background

Broadly defined, geospatial data is any data that includes locational or positional information about features in the dataset. Geospatial data provides the data foundation for applications of Geographic Information System (GIS) technology.

The development and maintenance of geospatial data is usually the most expensive component in the implementation of GIS technology. In most cases, this high initial investment is justifiable because of the powerful capabilities of the technology and the fact that, if appropriately maintained, the data will be useful for a very long period, and in many cases, for a wide range of applications.

Most geospatial datasets include numerous attributes and parameters that relate to data variables, methodologies and assumptions. Knowledge and understanding of the implications of these variables is a key to the appropriate utilization of that data. Without appropriate documentation, this specialized knowledge usually resides only in the memory of the GIS specialist(s) who developed the original data. Because of the power of the GIS technology, geo-spatial analysis is increasingly being used to develop and implement a wide range of public policy. In many cases, these public policy applications endure long past the availability of the GIS-specialist(s) who developed one or more of the original geospatial datasets upon which the public policy and its subsequent implementation are

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Data Security Standard

Category	**Security Architecture**
Title	**Data Security Standard**
Number	

Applicability

☑ State Government Agencies

□ All..Not Applicable

☑ **Excluding higher education institutions**..Standard

□ State Funded Entities - **All entities receiving state funding for matters covered by this document**...............Not Applicable

☑ Other: **All Public Entities**..............................Guideline

Definitions:

Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2).

Guideline - Adherence is voluntary.

Status: ☑ **Adopted** □ **Draft** □ **Other:________**

Dates:

Date:

Date Adopted by NITC: September 18, 2007

Other: Appendix A contact information revised on January 23, 2009

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

It is the responsibility of all State of Nebraska agencies to protect all information stored in electronic form against unauthorized access.

2.0 Purpose and Objectives

In the normal course of business operations information is gathered, stored and transmitted in electronic form. This information is normally required to provide public services or to carry out other state business responsibilities. Information collected may be of a nature deemed confidential to the business process being carried out and as such not open to sharing with any other entity. Certain types of data may also be deemed personal information. It is the objective of this policy to provide safeguards to protect that information.

Common methods of protecting information include, but are not limited to:

- Staff education
- Restricted data access and usage
- Administrative policies and procedures
- Data encryption
- Network encryption
- Account authorization
- Strong passwords
- Biometric authentication
- Physical security
- Network Firewalls
- Server hardening

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State Agencies

Each state agency will be responsible for ensuring that all information stored in an electronic manner is protected with appropriate safeguards in a manner consistent with this standard and any other applicable security policies.

Each state agency will designate a data owner for each application or system who will be responsible for assigning the data classification according to the sensitivity and criticality of the information in accordance with the NITC Security Officer Handbook, and making all decisions regarding controls, access privileges, and information management.

Each state agency is responsible for filing a Data Security Compliance Report with the Office of the CIO by October 31 of each year.

5.0 Related Documents

5.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
5.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)
5.3 Data Security Compliance Report – See appendix A
5.4 NITC Data Classification Standard (http://www.nitc.state.ne.us/standards/index.html)

6.0 References

6.1 State of Nebraska Records Management Act (Neb. Rev. Stat. § 84-1201-1227)
6.2 National Institute Standards and Technology (NIST) Special Publication, 800-53, revision 1, "Recommended Security Controls for Federal Information Systems". (http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf).
6.3 NSA (INFOSEC) Assessment Methodology (IAM) (http://www.iatrp.com/certclass.cfm)

Appendix A

Data Security Standard Compliance Report for ____,
(hereafter referred to as 'Agency').

I affirm that the Agency has performed an inventory of all Agency data, classified the data in accordance with the NITC Security Officer Handbook, and have implemented appropriate safeguards to protect the data from unauthorized access or disclosure.

____ ___________________________
Agency Director Date

Submit by October 31 to:

Office of the CIO
Attn: Information Security Officer
501 South 14th Street
Lincoln, NE 68509

NEBRASKA TECHNOLOGY COMMISSION

STANDARDS AND GUIDELINES

Information Security Policy

Category	Security Architecture
Title	**Information Security Policy**
Number	

Applicability

☑ State Government Agencies

□ All................................Not Applicable

☑ **Excluding** Higher Education institutions ....Standard

□ State Funded Entities - **All entities receiving state funding for matters covered by this document**..................Not Applicable

☑ Other: **All Public Entities** .... Guideline

Definitions:

Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of the NITC Technical Panel.

Guideline - Adherence is mandatory.

Status

☑ Adopted □ Draft □ Other

Dates

Date:
Date Adopted by NITC: September 18, 2007
Last Review Date:

TABLE OF CONTENTS

PURPOSE

The purpose of this Information Security Policy is to provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, availability and privacy of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the minimum safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

The Information Security Policy is based upon the ISO 27002 standard framework and is designed to comply with applicable laws and regulations; including the Records Management Act (Neb. Rev. Stat. § 84-1201 - 1227), however, if there is a conflict, applicable laws and regulations take precedence.

This Information Security Policy sets the direction, gives guidance, and defines requirements for information security processes and actions across agencies. This policy documents many of the security practices already in place in some agencies.

The primary objectives are to:

- effectively manage the risk of exposure or compromise to State resources;
- communicate the responsibilities for the protection of information;
- establish a secure, resilient processing environment;
- provide security controls for internally developed software to protect unauthorized access, tampering, or programming errors;
- provide a formal incident management processes; and
- promote and increase the awareness of information security.

SCOPE

This policy is applicable to State of Nebraska full time and temporary employees, third party contractors and consultants, volunteers and other agency workers (hereafter referred to as "Staff"). The Nebraska Information Technology Commission (hereafter referred to as the "NITC") is fully committed to information security and agrees that all staff or any other person working on behalf of the State of Nebraska have important responsibilities to continuously maintain the security and privacy of agency data.

This policy applies to all State Agencies, Boards and Commissions (hereafter referred to as "Agency"). Any agency may enact stronger security safeguard requirements, as necessary, to meet their individual business needs, State or Federal regulations. Where conflicts exist between this policy and an agency's policy, the more restrictive policy shall take precedence.

This Information Security Policy encompasses all systems, automated and manual, for which the State has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. This policy, subject to the provisions of the Records Management Act, applies to information in all forms, including but not limited to paper, microfilm, and electronic formats, created or used in support of business activities of the agency. This policy must be communicated to all staff that have access to or manage agency information.

Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this mandatory Information Security Policy. Published guidelines and standards reflect current practices and will be periodically reviewed and updated as necessary to meet changes in business needs, State or Federal regulations, or changes in technology implemented or supported by the State of Nebraska.

APPLICABILITY

The NITC has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for State agencies and educational institutions for information technology. This Information Security Policy will be implemented to ensure uniformity of information protection and security management across the different technologies deployed within an agency.

The Secretary of State (State Records Administrator) has statutory responsibility to establish standards, procedures, and techniques to assist agencies in identifying essential records, and guide them in the establishment of schedules for the creation, preservation, and disposal of such records.

POLICY

The components of this Information Security Policy encompass: 1) Operational Roles and Functional Responsibilities, 2) Management of the confidentiality, integrity and availability of State of Nebraska Information, 3) Personnel Accountability and Security Awareness, 4) Compliance, 5) Physical and Environmental Security, 6) Asset Classification, 7) Access Control, 8) Operational Management, and 9) System Development and Maintenance.

Section 1. Operational Roles and Functional Responsibilities

Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an internal information security infrastructure that ensures the confidentiality, availability, and integrity of the State's information assets.

State Agencies: Management will ensure that an information security organization structure is in place to:

- appoint, designate or hire an Information Security Officer to serve as the primary agency point of contact to the State Information Security Officer;
- implement information security policies, procedures and standards as necessary to meet security requirements imposed on the agency by federal, state or local regulations and as promulgated by the NITC;
- assign information security responsibilities;
- implement a security awareness program;
- monitor exposure and implement appropriate safeguards of information assets;
- monitor and implement changes to meet legal or regulatory requirements;
- respond to security incidents; and
- develop a process to measure compliance with this policy.

As required by this policy, an Agency Information Security Officer must be designated to oversee all security-related events and information. Depending on the agency's size and complexity, this role may be a fulltime position. The Agency Information Security Officer may report to the Agency Management.

Office of Chief Information Officer: The Chief Information Officer is the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the State of Nebraska. The State Information Security Officer, operating through the Office of the Chief Information Officer, performs as a security consultant to agencies and Agency Information Security Officers. The Office of the CIO may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Nebraska Information Technology Commission (NITC): The NITC is the owner of this policy with statutory responsibility to promote information security through adoption of policies, standards, and guidelines. The NITC develops strategies for implementing and evaluating the effectiveness of information security.

The **NITC Technical Panel**, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

For additional roles and responsibilities that an agency may adopt, see Addendum A.

Section 2. State of Nebraska Information

State information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies, standards, and practices must be implemented to ensure the confidentiality, integrity, and availability of State information is not compromised.

Management of the Confidentiality, Integrity, and Availability of State Information

The confidentiality, integrity, and availability of State of Nebraska information is critical to support an agency's business activities. Security controls provide the necessary physical, logical and procedural safeguards to protect State resources.

All information, regardless of the form or format, which is created, acquired or used in support of State of Nebraska's business activities, must be used for official business only. Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Information must be classified and protected based on its importance to business activities, risks, and security best practices. (See NITC Data Security Standard.)

Sharing Non-public Information Outside the Agency

For information to be released outside an agency or shared between agencies, a process must be established that, at a minimum:

- evaluates and documents the sensitivity of the information to be released or shared;
- identifies the responsibilities of each party for protecting the information;
- defines the minimum controls required to transmit and use the information;
- records the measures that each party has in place to protect the information;
- defines a method for compliance measurement;
- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the controls (Refer to Section 6. Asset Classification).

Non-public State information must not be made available through a public network without appropriate safeguards approved by the data owner(s). The agency must implement safeguards to ensure access control, and data protection measures are adequately protecting State information and logs are collected and protected against unauthorized access. Non-public information includes, but is not limited to:

- critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction or misuse could have a debilitating impact on health, welfare or economic security of the citizens and businesses of the State of Nebraska
- data that identifies specific structural, operational, or technical information, such as: mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities;
- personal identifying information as defined under Neb. Rev. Stat. § 87-802.

Section 3. Personnel Accountability and Security Awareness

The State of Nebraska provides information technology resources to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

Individual Accountability

Each user must understand his/her role and responsibilities regarding information security issues and protecting state information. Access to agency computer(s), computer systems, and networks where the data owner(s)has authorized access, based upon the "Principle of Least Privilege", must be provided through the use of individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc. Each individual is responsible for reasonably protecting against unauthorized activities performed with their UserID.

Associated with each UserID is an authentication token, such as a password or pin, which must be used to authenticate the person accessing the data, system or network. These authentication tokens or similar technology must be treated as confidential information, and must not be shared or disclosed. *(Refer to Section 7. Access Control and, NITC Individual Use Policy).*

Agency Accountability

All agency information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Each agency will follow established data classification processes in accordance with the NITC Security Officer's Handbook, best practices, State directives, and legal and regulatory requirements, as determined by the appropriate levels of protection and classification of that information. All information will be classified and managed based on its confidentiality, integrity, and availability characteristics as defined in the *NITC Security Officer Handbook*.

To ensure interruptions to normal agency business operations are minimized and critical agency business applications and processes are protected from the effects of major failures, each agency, in cooperation with the Chief Information Officer, must develop disaster recovery and business continuity plans that meet the recovery requirements defined by the agency. Preservation of critical data and software must be performed regularly and stored properly. Appropriate processes will be defined in the agency's recovery plan to ensure the reasonable and timely recovery of all information, applications, systems and security regardless of platform or physical form or format, should that information become corrupted, destroyed, or unavailable for a defined period. *(Refer to NITC Information Technology Disaster Recovery Plan Standard)*

To provide accountability regarding physical computing assets, each agency must maintain an up-to-date inventory of all State hardware and software, in accordance with DAS or agency fixed asset guidelines.

Including Security in Job Responsibilities

Specific security roles and responsibilities for those individuals responsible for information security must be documented. *(See Addendum A and Addendum B for specific roles and responsibilities).*

User Training

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the State. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. *(See NITC Individual Use Standard)*. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities. (See NITC Education, Training & Awareness Policy)

Separation of Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical.

Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.

Section 4. Compliance

Managing Compliance

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the State Information Security Officer. The failure to comply with this or any other security policy that may or may not result in the compromise of State information confidentiality, integrity, privacy, and/or availability may result in action as permitted by law, rule, regulation or negotiated agreement. Each agency will take appropriate steps necessary, including legal and administrative measures, to protect its assets and monitor compliance with this policy.

An agency review to ensure compliance with this policy must be conducted at least annually and each Agency management will certify and report the agency's level of compliance with this policy in accordance with the NITC Data Security Standard.

The State Information Security Officer may periodically review Agency compliance with this policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or systems which are the subject of the published policy or standard.

Monitoring

Consistent with applicable law, employee contracts, and agency policies, the Chief Information Officer reserves the right to monitor, inspect, and/or search at any time all State of Nebraska information systems. Since agency computers and networks are provided for business purposes, staff shall have no expectation of privacy of the information stored in or sent through these information systems. The Chief Information Officer additionally retains the right to remove from agency information systems any unauthorized material.

Only individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events on the State network. Network connection ports should be monitored for unknown devices and un-authorized connections.

Incident Response

Agencies must identify incident response procedures to promote effective response of security incidents, including procedures for information system failure, denial of service, disclosure of confidential information and compromised systems, according to the NITC Incident Response and Reporting Procedure for State Government.

To ensure quick, orderly, and effective responses to security incidents, all users of agency systems must be made aware of the procedure for reporting security incidents, threats or malfunctions that may have an impact on the security of State information. ***Users must not attempt to prove a suspected weakness unless specifically authorized by the agency to do so*.**

Note: Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation.

Section 5. Physical and Environmental Security

Physical Security Perimeter

Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information, and implement reasonable and appropriate hardening measures to prevent and detect unauthorized access, theft, damage or interference.

Based on the threat and risk assessment, a multi-layered physical security perimeter must be established in agency environments where information or information assets are stored or where operational data centers, network wiring closets, or telephony connection equipment exists, or where printers that print confidential or sensitive information may be printed, and any other location where information may be in use or stored, such as file cabinets, microfiche storage areas, etc. The security layers create a security perimeter that would require multiple methods of access control to gain entry. These layers could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office, or other physical barrier.

To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities.

Asset Security

Computer assets must be physically protected from physical and environmental hazards to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may be necessary for electrical supply and uninterruptible power, fire protection and suppression, air and humidity controls, and cabling infrastructure in data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

Secure Disposal or Re-use of Storage Media and Equipment

Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the State of Nebraska. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g. tape, diskette, CDs, DVDs, USB drives, cell phones, memory sticks, digital copiers/printers/scanners with data storage capabilities) regardless of physical form or format containing sensitive information (Refer to Section 6 Asset Classification) must be physically destroyed or securely overwritten when the data contained on the device is no longer required under the provisions of the Records Management Act.

Clear Screen

To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.

Section 6. Asset Classification

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the State of Nebraska, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of State data in compliance with this policy and the agency Records Retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, etc.

Data owned, used, created or maintained by the State is classified into the following four categories:

- Public
- Internal Use Only
- Confidential
- Highly Restricted

(See NITC Security Officer Handbook)

Section 7. Access Control

To preserve the confidentiality, integrity and availability, state information assets must be protected by logical and physical access control mechanisms.

Logon Banner

Logon banners must be implemented on all workstations, servers and laptops to inform users that the system is for official agency use, or other approved use consistent with agency policy, and that user activities may be monitored, and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

User Account Management

A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities. (See NITC Identity and Access Management Standard and NITC Acceptable Use Policy State Data Communication Network)

Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.

Privileged Accounts Management

The issuance and use of privileged accounts will be restricted and controlled. Processes must be developed to ensure that users of privileged accounts are monitored, and any suspected misuse is promptly investigated.

All individuals requiring special privileges (programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (UserID) so activities can be traced to the responsible user. UserIDs must not give any indication of the user's privilege level, e.g., supervisor, manager, administrator, etc. (See NITC Remote Administration of Internal Devices Standard).

User Password Management

Passwords are a common means of authenticating a user's identity to access information systems or services. Passwords must be implemented to ensure all authorized individuals accessing agency resources follow the NITC Password Standard.

Password management controls should be implemented, where technically or operationally feasible, to provide a reliable, effective method of ensuring the use of strong passwords.

Network Access Control

Access to an agency's trusted internal network must require all authorized users to authenticate themselves through the use of an individually assigned User ID and an authentication mechanism (e.g., password, token, smart card, etc.). Network controls must be developed and implemented that ensure authorized users can access only those network resources and services necessary to perform assigned job responsibilities.

User Authentication for External Connections (Remote Access Control)

In the special case where software, servers, storage devices or other computer equipment has the capability to automatically connect to a vendor (e.g. to report problems or suspected problems), the Agency Information Security Officer or designee must conduct a risk assessment prior to establishing access to ensure that connectivity does not compromise the state or other third party connections.

(See also Section 8. Operational Management, External Connections and NITC Remote Access Standard)

Segregation of Networks

When the state network is connected to another network, or becomes a segment on a larger network, controls must be in place to prevent users from other connected networks access to the agency's private network. Routers or other technologies must be implemented to control access to secured resources on the trusted state network.

Detailed maps of agency physical and logical network connections should be available to the State Information Security Officer.

Operating System

Access to operating system code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities.

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared UserID/password for a group of users or a specific job can be used. Approval by Agency Information Security Officer or designee must be documented in these cases. The approval process must include the State Information Security Officer. Additional compensatory controls must be implemented to ensure confidentiality and accountability is maintained *(See Section 3. Personnel Accountability and Security Awareness, Individual Accountability).*

Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

Application Access Control

Access to systems and business applications must be restricted to those individuals who have a business need to access those resources in the performance of their job responsibilities.

Monitoring System Access and Use

Activities of information systems and services must be monitored and events logged to provide a historical account of security related events. Agencies will implement appropriate audit logs to record events, exceptions and other security-relevant events. The Agency Information Security Officer or designee will regularly review logs for abuses and anomalies. Logs will be kept consistent with Record Retention schedules developed in cooperation with the State Records Administrator and agency requirements to assist in investigations and access control monitoring.

Section 8. Operational Management

All information processing facilities must have detailed documented operating instructions, management processes and formal incident management procedures authorized by agency management and protected from unauthorized access. Where an agency provides a server, application or network services to another agency, operational and management responsibilities must be coordinated by both agencies.

Network Management

The Office of the Chief Information Officer and agencies will implement a range of network controls to ensure the integrity of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. If there is a business need, additional measures to ensure the confidentiality of the data will also be implemented. The Office of the Chief Information Officer will ensure that measures are in place to mitigate any new security risks created by connecting the state network to a third party network. All direct connections to the

State network and direct connections between agencies must be authorized by the Office of the Chief Information Officer.

Where an agency has outsourced a server or application to a third party service (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board or designee will perform the security review on behalf of all Agencies.

Additions or changes to network configurations, including through the use of third party service providers, must be reviewed and approved through the Office of the Chief Information Officer's change management process.

Cooperation Between Organizations

The Agency Information Security Officer should maintain contact lists of both internal and external contacts and service providers. These lists should be organized to quickly facilitate security-related events and investigations and should detail the agency management staff authorized to make decisions regarding security-related events.

Membership in security-related organizations may provide valuable insight into the ongoing practices of security administration; however, the release of information regarding State security events and issues is strictly prohibited without Office of the Chief Information Officer prior approval.

Penetration Testing, Intrusion Testing, and Vulnerability Scanning

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to agency penetration testing, intrusion testing, and vulnerability scanning.

- All servers will be scanned for vulnerabilities and weaknesses by the Office of the Chief Information Officer before being installed on the State network. For both internal and external systems, scans will be performed at least annually or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. The frequency of additional scans will be determined by the agency and the data owner(s), depending on the criticality and sensitivity of the information on the system.

- All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred.

- Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing, and vulnerability scans will be reviewed in a timely manner by the State Information Security Officer. Any vulnerability detected will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the State Information Security Officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing and vulnerability scanning must be coordinated by both entities.

Any penetration or intrusion testing or vulnerability scanning, other than that performed by State Information Security Officer must be conducted by individuals who are authorized by the State Information Security Officer and who have requested and received written consent from the Office of the Chief Information Officer at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed at all times to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

External Connections

Direct connections between the State network and external networks must be implemented in accordance with the *NITC Remote Access Standard*. Connections will be allowed only when external networks have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented to protect state resources. A risk analysis should be performed to ensure that the connection to the external network would not compromise the state's private network. Additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) may be implemented between any third party and the state. All external connections will be reviewed on an annual basis.

Third party network and/or workstation connection(s) to the state network must have an agency sponsor and a business need for the network connection. An agency non-disclosure agreement may be required to be signed by a legally authorized representative from the third party organization. In addition to the agreement, the third party's equipment must also conform to the state's security policies and standards, and be approved for connection by the Office of the Chief Information Officer.

Any connection between agency firewalls over public networks that involves sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

(See also Section 7. Access Control, User Authentication for External Connections)

Portable Devices

All portable computing devices (notebooks, USB flash drives, PDA's, laptops and mobile phones) and information must be secured to prevent compromise of confidentiality or integrity. No device may store or transmit sensitive information without suitable protective measures that are approved by the agency data owner(s).

Special care must be taken to ensure that information stored on the device is not compromised. Appropriate safeguards must be in place for the physical protection, access control, cryptographic technique, back up, virus protection, and properly connected to the State network.

Devices storing sensitive and/or critical information must not be left unattended and, where possible, must be physically locked away, or utilize special locks to secure the equipment.

Employees in the possession of portable devices must not check these devices in airline luggage systems. These devices must remain in the possession of the traveler as hand luggage unless restricted by Federal or State authorities.

Server Hardening

In order to protect State resources, agencies must remove all unnecessary software and disable services in accordance with NITC Minimum Server Configuration Standard.

System Planning

Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of resources. Storage and memory capacity and other hardware requirements must be monitored and future requirements projected to ensure adequate processing and storage capabilities are available when needed. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Protection against Malicious Code

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the State environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk. For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published.

Software Maintenance

All installed software must be maintained at a vendor-supported level to ensure accuracy and integrity. Maintenance of agency-developed software must follow the State's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner as defined by the Agency.

Wireless Networks

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security risks, if not addressed correctly, could expose state information systems to a loss of service or compromise of sensitive information. Everything that is transmitted over the radio waves (wireless devices) can be intercepted. This represents a potential security issue. Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of State data and information systems associated with the use of wireless network access technologies in accordance with the NITC Wireless Local Area Network Standard.

No wireless network or wireless access point will be installed without the written approval of the Office of the Chief Information Officer.

Communications

Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the state E-mail system are a visible representative of the state and must use the system in a legal, professional and responsible manner. Users must comply with this policy, the Records Management Act, and be knowledgeable of their responsibilities as defined in NITC Secure E-Mail for State Agencies.

Telephones and Fax Equipment

Communication outside the state telephone system for business reasons is sometimes necessary, but it can create security exposures. Employees should take care that they are not overheard when discussing sensitive or confidential matters; avoid use of any wireless or cellular phones when discussing sensitive or confidential information; and avoid leaving sensitive or confidential messages on voicemail systems. (See Section 6. Asset Classification and NITC Use of Computer-based Fax Services by State Government Agencies)

Modem Usage

Connecting dial-up modems to computer systems on the state network is prohibited unless a risk assessment is performed, risks are appropriately mitigated, and the Office of the Chief Information Officer approves the request.

Section 9. System Development and Maintenance

To ensure that security is built into information systems, security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to, and documented as part of the overall business case for the system. To ensure this activity is performed, the Agency Information Security Officer or designee must be involved in all phases of the System Development Life Cycle from the requirements definition phase, through implementation and eventual application retirement.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, and included in the agency's security standards documents. The security measures that are implemented must be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

Agencies should follow the latest "best practices" in secure coding techniques as identified in NIST guidelines, OWASP principles, etc.

System Acceptance

The security requirements of new systems must be established, documented and tested prior to their acceptance and use. Agency Information Security Officer or designee will ensure that acceptance criteria are utilized for new information systems and upgrades. Acceptance testing will be performed to ensure security requirements are met prior to the system being migrated to the production environment.

Separation of Development, Test and Production Environments

Development software and testing tools can cause serious problems to the production environment if separation of these environments does not exist. Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. Separation must also be implemented between development and test functions. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

- access to compilers, editors and other system utilities must be removed from production systems when not required; and
- logon procedures and environmental identification must be sufficiently unique for production testing and development.

Risk Assessment

Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Internet (Web) and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to:

- address the business risks and develop a data classification profile to help to understand the risks;
- identify security measures based on the criticality and data sensitivity and protection requirements;
- identify and implement specific controls based on security requirements and technical architecture;
- implement a method to test the effectiveness of the security controls; and
- identify processes and standards to support changes, ongoing management and to measure compliance.

Input Data Validation

An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. The checks that are performed on the client side must also be performed at the server to ensure data integrity. Checks will be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. A process should be set up to verify and correct fields, characters, and completeness of data and range/volume limits.

Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into systems to prevent or stop an incorrect program from running. Application design must ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity.

Message Integrity

Message integrity must be considered for applications where there is a security requirement to protect the message or data content from unauthorized changes (e.g. electronic funds transfer, EDI transactions, etc.) Encryption techniques should be used as a means of implementing message integrity. *It should be noted that message integrity does not protect against unauthorized disclosure.*

Cryptographic Controls

Use of encryption for protection of high-risk information should be considered when other controls do not provide adequate protection. The decision to use encryption should be based on the level of risk of unauthorized access and the sensitivity of the data to be protected. Consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of a cryptographic key would cause all information encrypted with that key to be considered at risk.

Protection of System Test Data

Test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application. Production data may not be used for testing unless all personally identifiable information is removed.

Once test data is developed, it must be protected and controlled for the life of the software, system or application. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Protection of Source Code

Access to source code libraries for both agency business applications and operating systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

Change Control Management

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.

DOCUMENT CHANGE MANAGEMENT

Requests for changes to this policy must be presented to the State Information Security Officer. If the State Information Security Officer agrees to the change, he or she will formally draft the change and have it reviewed and approved through the NITC normal policy approval process. Each Agency Information Security Officer will be responsible for communicating the approved changes to their organization.

This policy and supporting policies and standards will be reviewed at a minimum on an annual basis.

CONTACT INFORMATION

Questions concerning this policy may be directed to State Information Security Officer, or (402) 471-7031.

REPEAL

The Information Security Management Policy, Access Control Policy, Disaster Recovery Policy, and Network Security Policy, adopted on January 23, 2001, are repealed.
(http://nitc.ne.gov/tp/workgroups/security/security_policies.html.)

DEFINITIONS

Agency: State agencies, boards and commissions are collectively referred to as 'agency' throughout this document.

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security information to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user

Biometrics: Refers to the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.

Business Risk: This is the combination of sensitivity, threat and vulnerability.

Change Management Process: A business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that changes will perform as expected, with no unexpected repercussions.

Chief Information Officer: The Chief Information Officer is responsible for vision, strategy, direction, and oversight for Information Technology for State of Nebraska. The Chief Information Officer reports to the Governor, is a member of the Governor's cabinet, and is a member of the Nebraska Information Technology Commission, which oversees and legislates IT standards and policy as empowered by law.

Classification: The designation given to information or a document from a defined category on the basis of its sensitivity.

Computer: All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and systems, databases, memory, Internet service, information systems, laptops, Personal Digital Assistants and accompanying equipment used to support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Critical: A condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media, including all records as defined by the Records Management Act.. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Data Owner: An individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the State of Nebraska's business objectives.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Executive Management: The person or persons charged with the highest level of responsibility for an Agency (e.g. Agency Director, CEO, Executive Board, etc.).

External Network: The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.

Family Educational Rights and Privacy Act (FERPA): Federal law regarding the privacy of educational information. For additional information visit: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Gramm-Leach-Bliley Act (GLB): Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Guideline: An NITC document aims to streamline a particular process that Agency compliance is voluntary.

Health Insurance Portability Accountability Act (HIPAA): A Congressional act that addresses the security and privacy of health data. For additional information visit: http://www.hhs.gov/ocr/hipaa/

Host: A system or computer that contains business and/or operational software and/or data.

Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the State.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information Technology Resources: Hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, which facilitates data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

Internal Network: An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometimes masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

Nebraska Information Technology Commission (NITC): The governing body, set forth by the State of Nebraska Legislature. See http://www.nitc.state.ne.us/

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Information: Personal information means any information concerning a person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Policy: An NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the State of Nebraska

Principle of Least Privilege: A framework that requires users be given no more access privileges (read, write, delete, update, etc.) to systems than necessary to perform their normal job functions, and those privileges be granted no longer than the time required to perform authorized tasks.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Private Information: Private Information means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number; or
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The User ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator, etc.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this policy.

Records Officer: The agency representative from the management or professional level, as appointed by each agency head, who is responsible for the overall coordination of records management activities within the agency.

Records Management Act: The governing statute, set forth by the State of Nebraska Legislature. Neb. Rev. Stat. § 84-1201 through § 84-1228

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Separation of Duties: A concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

Sensitive Information: Disclosure or modification of this data would be in violation of law, or could harm an individual, business, or the reputation of the agency.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Sniffer: Monitoring network traffic.

Staff: Any State of Nebraska full time and temporary employees, third party contractors and consultants who operate as employees, volunteers and other agency workers.

Standard: Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detail factors.

State: The State of Nebraska.

State Information Security Officer: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security Architecture Workgroup. Responsibilities include creating and maintaining polices for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer's.

State Network: The State of Nebraska's internal, private network, e.g. the State's 10.x.x.x address space.

State Records Administrator: The Secretary of State is the State Records Administrator. The Secretary of State establishes and administers the records management program for all state agencies.

System(s): An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

System Development Life Cycle: A software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

Third Party: Any non-agency contractor, vendor, consultant, or external entity, etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Token: A device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

Trojan Horse: Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access Or Privileges: Insider or outsider who gains access to network or computer resources without permission.

User: Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Vulnerability: A weakness of a system or facility holding information that can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

World Wide Web (WWW): A hypertext-based system designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and Internet Explorer are two of the most popular web browsers.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

INDEX

ADDENDUM A

Operational and Functional Responsibilities

Data Owner: An individual or a group of individuals designated by an agency that represents the agency concerning the data the agency owns and tools the agency uses on the data. Data owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). Data owners also communicate to the Agency Information Security Officer the legal requirements for access and disclosure of their data. Data owners must be identified for all agency information assets and assigned responsibility for the maintenance of appropriate security measures such as assigning and maintaining asset classification and controls, managing user access to their resources, etc. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

Data Custodian: An individual or a group of individuals designated by the Data owner who will be responsible for maintaining and protecting the data. This role is typically filled by the IT department, and the duties include performing regular backups of the data, periodic validating the integrity of the data, restoring data from backup media, retaining records of activity, and fulfilling the requirements specified in this Security Policy and NITC standards and guidelines that pertain to information security and data protection.

Agency Information Security Officer: The Agency Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information security policies and standards. The Agency Information Security Officer is responsible for providing direction and leadership to the agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The Agency Information Security Officer is responsible for investigating all alleged information security violations. In this role, the Agency Information Security Officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The agency Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives. *(For more detail, see Addendum B, Role and Responsibilities of the Agency Information Security Officer.)*

Security Administrators: When such an individual or individuals exist, the individual or individuals will work closely with the Agency Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all UserIDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal Security Administration function does not exist, the organization or staff responsible for the security administration functions described above will adhere to this policy.

Information Technology (IT) Management: IT management has responsibility for the data processing infrastructure and computing network which support the data owners. It is the responsibility of IT management to support the Information Security Policy and provide resources needed to enhance and maintain a level of information security control consistent with the agency's Information Security Policy.

IT management has the following responsibilities in relation to the security of information:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the agency's business;
- ensuring the proper controls of information are implemented for which the agency's business have assigned ownership responsibility, based on the agency's classification designations;
- ensuring the participation of the Agency Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets;
- ensuring that appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility;
- ensuring that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.

NITC Technical Panel: The NITC Technical Panel, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

State Records Administrator: The State Records Administrator establishes and administers, within and for state and local agencies, (1) a records management program which will apply efficient and economical methods to the creation, utilization, maintenance, retention, preservation, and disposal of state and local records, (2) a program for the selection and preservation of essential state and local records, (3) establish and maintain a depository for the storage and service of state records, and advise, assist, and govern by rules and regulations the establishment of similar programs in local political subdivisions in the state, and (4) establish and maintain a central microfilm agency for state records and advise, assist, and govern by rules and regulations the establishment of similar programs in state agencies and local political subdivisions in the State of Nebraska. Neb. Rev. State § 84-1203

ADDENDUM B

Role and Responsibilities of the Agency Information Security Officer

The Agency Information Security Officer is responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of information security policies, standards, procedures, and other control processes that meet the business needs of the agency;
- provide consultation on the various agency computing platforms;
- work closely with security administration or those serving in that function to ensure security measures are implemented that meet policy requirements;
- evaluate new security threats and counter measures that could affect the agency and make appropriate recommendations to the State Information Security Officer and other appropriate management to mitigate the risks;
- review and approve all external network connections to the agency's network;
- provide consultation to the agency management with regard to all information security;
- investigate and report to appropriate agency management and the State Information Security Officer according to the NITC Incident Reporting Policy;
- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate information security awareness and education to all agency
- staff, and where appropriate third party individuals;
- be aware of laws and regulations that could affect the security controls and classification requirements of the agency's information;

The mission of the Information Security Function is to:

- develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the agency;
- provide information security recommendations to the agency regarding security threats that could affect the agency's computing and business operations, and make recommendations to mitigate the risks associated with these threats;
- assist management in the implementation of security measures that meet the business needs of the agency;
- develop and implement security training and awareness programs that educate agency employees, contractors and vendors with regard to the agency's information security requirements;
- investigate and report to management breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained;
- participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the agency's business and the security controls, in the event of an extended period of computing resource unavailability;