CITY OF CHULA VISTA

CITY OF CHULA VISTA

Telecommunications Master Plan

Magellan ADVISORS

www.MAGELLAN-ADVISORS.com

FINAL 2020

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

Acknowledgements

Magellan Advisors wishes to thank the City of Chula Vista for the opportunity to assist with this important work. We would like to thank City leadership and staff for the vision, time, and thoughtful input they invested in providing the development of this Plan.

MUNICIPAL AND COMMUNITY ANCHORS

City of Chula Vista | City of Chula Vista Information Technology Department | City of Chula Vista Department of Public Works | Chula Vista Police Department | Chula Vista Law Department | Chula Vista Community Services | Chula Vista Finance Department | Chula Vista Fire Department | Chula Vista Human Resources Department | Chula Vista Transportation Department| Chula Vista Development Services | Chula Vista Economic Development | Chula Vista Office of Sustainability | Port of San Diego | Madaffer Enterprises, Inc.

1. Executive Summary

1.1 ABOUT CHULA VISTA

The City of Chula Vista ("Chula Vista", or "the City") is the second largest city in the San Diego metropolitan area, the seventh largest city in Southern California, and the eleventh largest city in the state of California. The City encompasses approximately 50 square miles in southern San Diego County with a population of approximately 274,000. Located just 7.5 miles (12.1 km) from downtown San Diego and 7.5 miles (12.1 km) north of the Mexican border in the South Bay region of the metropolitan area, the city is at the center of one of the richest economic and culturally diverse zones in the United States. The City consists primarily of residential neighborhoods, delineated in western and eastern Chula Vista with Interstate 805 as the demarcation line. The western part is the older portion of the City, with a primarily grid type layout on mostly flat terrain. The eastern part is primarily made of master planned communities, with rolling hills and newer infrastructure.

Chula Vista is growing at a fast pace, with major developments taking place in the Otay Valley near the U.S. Olympic Elite Athlete Training Center and Otay Lake Reservoir. Thousands of new homes have been built in the Otay Ranch, Lomas Verdes, Rancho Del Rey, Eastlake and Otay Mesa areas. The City, in conjunction with the Port of San Diego, is supporting the Bayfront Development, a major mixed-use development area on the coastal west side of the City. The Millenia Project is a mixed-use urban development project which includes upscale apartments, homes, and business space. On the east side, the City is dedicating 375 acres to the University and Innovation District, to which the City aims to recruit and collocate a unique mix of academic partners in an urban, mixed-use setting; the area will provide a collaborative learning and research environment for engaging both academic and corporate entities with a focus on cross-border economic, social, and cultural studies. In addition, the City is actively planning the revitalization of Third Avenue and other parts of the more-developed western side of the City.

The City of Chula Vista is a charter City and operates under a Council-Manager form of government. The City employs approximately 1,300 full- and part-time employees in various disciplines including standard office environments. The City is considered a full-service City with Fire, Police, and Public Works (sewer) services.

1.2 ABOUT THIS STUDY

The City of Chula Vista has embarked on an ambitious Smart Cities vision. The goals of the Smart Cities vision are to:

- Connect all City facilities, providing a secure, cost effective, redundant and flexible network infrastructure to meet current and future data, video and voice communications needs;
- Provide a network infrastructure to enable the City to control its telecommunications costs, implement smart city initiatives and encourage economic development;

- Provide a network infrastructure which enables applications and services, and facilitates innovation and economic development within the City, including the Bayfront, Millenia, and University & Innovation areas;
- Provide timely, accurate data to centralized locations from myriad sources including IoT devices, mobile field units (for Police, Fire, Public Works) and other infrastructure to maximize efficiency and enable timely, accurate business management decisions;
- Connect citizens to City services and provide access to data which will allow citizens to be more connected to their government. Further, the City envisions significantly reducing the "digital divide" by providing access to the internet and City digital services to underserved areas;
- Where practical, develop Public - Private partnerships to further the Smart Cities vision.

In 2018, the City retained Magellan Advisors ("Magellan") to develop this Telecommunications Master Plan ("TMP") to focus on the development of a fiber and telecommunications infrastructure to support the City's Smart Cities vision. Along with a plan for network infrastructure for the City, Magellan provides advice and policies, organization assessment, and frameworks for the City to enable its Smart Cities vision.

Magellan reviewed several existing City reports which had been previously commissioned, including:

- 2017 Chula Vista Smart Bayfront, Energy Technologies Assessment – Black and Veatch
- 2017 Chula Vista Smart Bayfront, Communications and Smart Infrastructure – Black and Veatch
- 2018 Smart Cities Technology Analysis, Recommendations for Bayfront – Black and Veatch
- 2018 Baseline Network Assessment Report (IT) – NIC Partners
- 2017 Smart City Strategic Action Plan – (Maddafer)
- 2017 Traffic Signal Communications Master Plan
- 2016 Chula Vista Fiber Optic System Assessment – Black and Veatch

Magellan conducted a two-day on-site kickoff, coordinating through Information and Technology Services (ITS) Director Edward Chew. Many department heads were interviewed on current situation, needs and plans. Department heads from Economic Development, Law, Finance, Sustainability, Public Works, Traffic, and others participated.

Magellan also requested the City to provide many GIS data layers for analysis and to support possible fiber route planning which were provided by ITS and Traffic Division and uploaded to Magellan's GISCloud instance for the City of Chula Vista.

1.3 TELECOMMUNICATIONS MASTER PLAN (TMP) SUMMARY

In this Executive Summary, Magellan provides a synopsis of the findings and recommendations in the Telecommunications Master Plan (TMP).

1.3.1 Core Infrastructure and LAN/MAN Opportunities

This section details the efforts of the Information and Technology Services ("ITS") and Traffic Control ("Traffic") divisions on their planning initiatives to upgrade the Chula Vista networks and fiber networks. Traffic is already upgrading some traffic signals to connect to the Traffic Management Center (TMC) via fiber, and 24 signals are currently connected in this way. The section details the necessary attributes of a robust fiber network, defining scalability, performance, inter-operability, reliability, multi-purpose, security and operations traits, along with statements on required staff to support such a network. It outlines the several benefits of having a dedicated fiber network, including improved operational and financial control, and reduced reliance on third-party operators.

The analysis then moves to design and phased implementation of a Citywide fiber network. The phased proposal is to construct three rings, first in the west and expanding eastward. The first ring is implemented in three phases: first, the fiber backbone ring, second, connecting traffic signals along the network via new fiber, and third, connecting City building sites to the fiber network for operations. The second ring connects to the first, and is itself implemented in two phases: first, the backbone ring, and then connecting traffic signals to new fiber. The third ring completes the proposed network, connecting all remaining traffic signals to the network.

Table 1-1 Network Construction Phases

Phase	Recommendation	Phase Scope, Description
1	Required	Backbone Ring 1, Connecting Data Centers and Aggregation Sites
2	Required	Traffic Network Connecting to Ring 1
3	Required	Laterals Connecting City Sites to Ring 1
4	Contingent	Backbone Ring 2 and Laterals to City Sites
5	Contingent	Traffic Network Connecting to Ring 2
6	Contingent	Backbone Ring 3 (Blue) and Remaining Traffic Network

Implementation of the second and third rings are contingent on availability of complete funding for all components of a specific phase.

Conceptually, the completed network schematic is as follows:

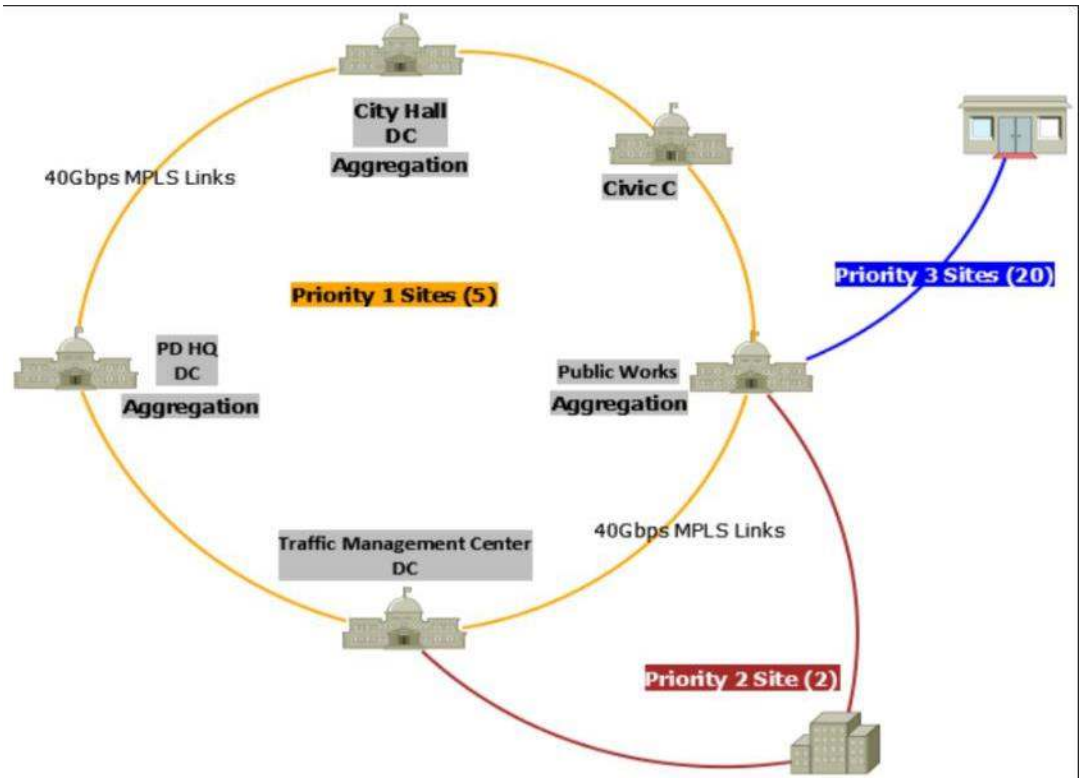


Figure 1-1 Chula Vista Conceptual Network Architecture (Three Rings)

The implementation of the network is phased, creating a series of rings, which permit communications traffic to have redundant paths back to City data centers.

The first ring, in the western part of the City, connects the City data centers with fiber along Main Street in the south, turning north along 4th Avenue, then east along E Street, before turning south along 2nd Avenue. At E H Street, the ring runs east before turning south again at E Hilltop Drive, heading east at E L Street, crossing over the I-805 onto Telegraph Canyon Road before turning south onto Brandywine Avenue. before closing the loop back on Main Street. This ring connects the four Priority 1 sites in a loop, permitting traffic to flow in either direction to access any City data center. In the second and third Phases, the ring also connects 16 other City buildings and 21 traffic signals. This westside ring covers the more densely populated part of Chula Vista, bringing fiber connectivity to most City buildings and the possibility for dark fiber leasing to commercial providers and other entities.

Figure 1-2 Ring 1 (Phases 1-3) Westside Ring

The second ring breaks off from the first ring at E H Street, heading east to Proctor Valley Road, turning south along Hunte Parkway until it turns west at Olympic Parkway, merging back onto E Palomar Street where it reconnects with the first ring at Brandywine. This ring connects the remaining planned 7 City buildings and 8 additional traffic signals.

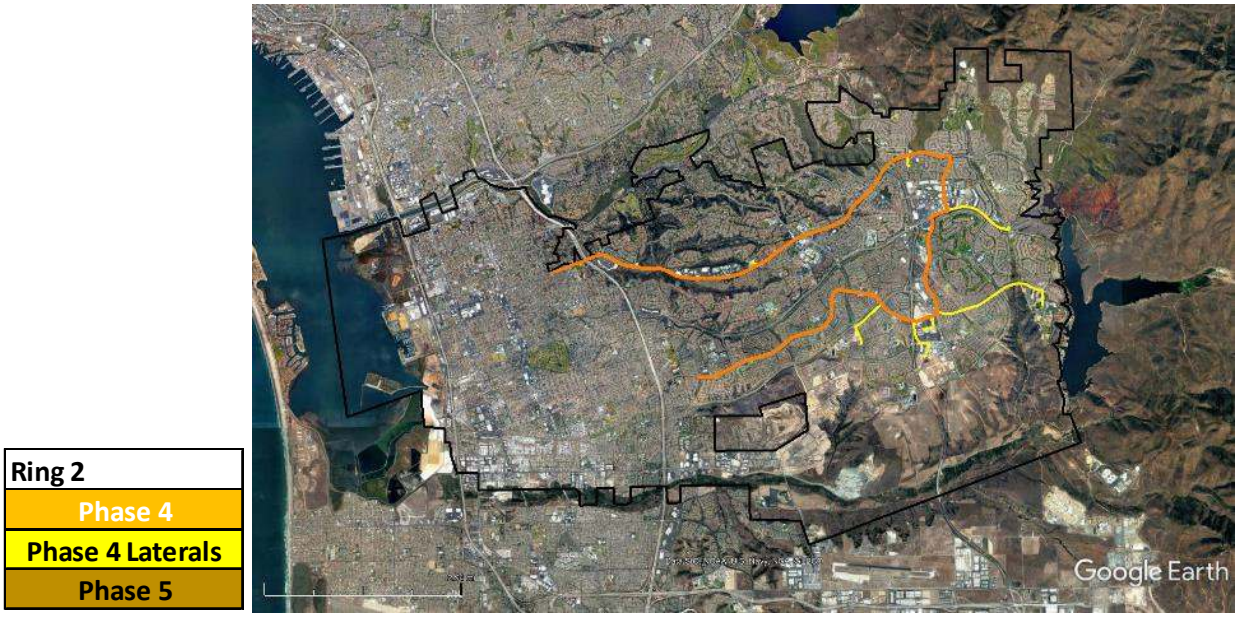


Figure 1-3 Ring 2 (Phases 4-5) Northeast Ring

The third ring in the far east of the City continues south along Hunte Parkway, extending south along 125, before heading west along the southern part of the City, where it reconnects with

Main Street. This ring enables growth in the southeast part of the City, and connects 5 additional traffic signals.

Figure 1-4 Ring 3 (Phase 6) Southeast Ring

Phase 1 creates a physical ring consisting of 288-count fiber diversely routed to connect City IT, Police Department headquarters, Traffic Management Center, and Public Works. This physical ring connects to core switches at each site to provide both protected high-speed transport between the data centers and remote site aggregation for end user access to the applications and storage. In addition to remote City sites, the ring also aggregates the traffic control networks, surveillance systems, and future Smart City components. (See Appendix C for a complete list of named sites associated with each ring.)

Following is an example, details in the TMP include a map of the proposed routes along with summary metrics for the construction. Phase 1 is included here; the remaining five phases are in the body of the report.

Phase 1 includes 14.3 route miles of fiber consisting of the primary backbone fiber ring and connection of four sites, including City IT, Traffic Management Center, Police Headquarters, and Public Works. All four buildings are designated as priority 1 sites.

Figure 1-5 Phase 1 Route Map

Phase 1

Phase 2 follows the Traffic Signal Communications Master Plan ("TSCMP") to construct fiber for the traffic signals networks in downtown Chula Vista. The traffic signals networks could be deployed in physical rings or daisy chained configurations, depending on available equipment budget and fiber topology. Each group of signal controllers terminates to the aggregation switches on the transport ring for connectivity to the primary Traffic Management Center.

Phase 3 constructs fiber to connect sixteen (16) of the twenty-seven (27) City sites, including Traffic Center and Civic Center B, using 24-count laterals from each site to the aggregation switches on the transport ring. This would migrate the majority of City sites to City-owned fiber and allow the disconnection of monthly recurring leased services to those sites.

Phase 4 constructs a second physical fiber ring connecting sites and traffic signals networks in the northern half of the City. This ring would be used to aggregate City sites and traffic signals networks to the primary ring for termination into one or more of the aggregation sites. In addition, 24-count laterals would be constructed to the remaining seven remote City sites.

Phase 5 constructs the networks serving the northern traffic signals and terminates them to the aggregation sites on the primary ring for connectivity to the Traffic Management Center.

Phase 6 constructs a third physical ring connecting the southern half of the City, providing future fiber connectivity as growth occurs. The remaining traffic signals network points would also be transported by this ring to the aggregation sites for connectivity to the Traffic Management Center.

For the six phases, construction costs are almost directly proportional to the lengths of proposed fiber segments, based on Magellan's design. The following table summarizes core and lateral distances by phase:

Table 1-2 Summary of Fiber Network Metrics, by Ring, by Phase

		Core / Backbone		Laterals / Distribution		Core + Laterals	
Ring	Phase	Linear feet	Linear miles	Linear feet	Linear miles	Linear feet	Linear miles
1	1	73,371	13.90	2,539	0.48	75,910	14.38
1	2		0.00	112,855	21.37	112,855	21.37
1	3		0.00	35,953	6.81	35,953	6.81
2	4	70,343	13.32	31,332	5.93	101,675	19.26
2	5		0.00	81,280	15.39	81,280	15.39
3	6	32,953	6.24	17,971	3.40	50,924	9.64
		176,667	33.46	281,930	53.40	458,597	86.86
		38.52%		61.48%			

Magellan provides this order of magnitude estimate of design, engineering, construction, project management, construction management, and engineering costs, along with a contingency, for the three rings and six phases. Total costs for the entire construction effort, including contingency, are estimated at $20.03 million, as follows:

- Labor and Materials: $16.51 million;
- Contingency on L&M: $1.651 million (at 10%);
- Design and Engineering: $573K;
- Construction Management" $480K over three construction waves;
- Project Management: $384K over three construction waves;
- Equipment and Electronics: $435K, including 20% professional services for installation.

Table 1-3 Estimated Engineering, Construction, Management, and Equipment Costs

Ring	Phase(s)	Sites	Labor & Material	10% Contingency	Design and Engineering	Total Const, Des & Eng	Const Mgt	Project Mgt	Equipment *	Total
1 (Req)	1,2,3	20	7,916,462	791,646	238,073	8,946,181	180,000	144,000	283,010	**9,553,191**
2 (Cont)	4,5	7	6,657,756	665,776	228,248	7,551,779	180,000	144,000	87,080	**7,962,859**
3 (Cont)	6	0	1,932,937	193,294	106,925	2,233,156	120,000	96,000	65,310	**2,514,466**
		Totals:	**16,507,154**	**1,650,715**	**573,246**	**18,731,116**	**480,000**	**384,000**	**435,400**	**20,030,516**
			* = Includes professional services for installation							
			(Req = Required; Cont = Contingent on Funding)							

Although construction of the three backbone rings must precede the remote site and traffic signals connecting to them, the six phases are operationally independent of each other. Each phase can be implemented over three to twelve months, depending on the City's financing strategy. In addition, construction of the Phase 2, 3, and 5 remote site and traffic signal connections can be extended across multiple years if necessary, by maintaining the existing leased telecom services during the term of construction.

Magellan recommends the following as next steps for examining the proposed fiber network:

- Conduct Complete Engineering Design for Fiber Network.
- Construct Ring 1 (Phases 1-3) of Network – including all 5 Priority 1 sites and 20 City building sites
- Connect City Data Centers Along Primary Ring – including City Hall, at Civic Center Building A, and at Public Works Aggregation site.
- Centralize Network Management and Security – with ITS managing fiber network, while permitting Police Department and Traffic to manage their own user bases and applications running on the network.
- Integrate Traffic Control Networks to New Cisco Technical Infrastructure
- Collocate to Commercial Data Center for Direct Access to IP Service Providers

As currently planned, without commercialization of the network, there are no direct revenues to the City as a result of building this network; all the benefits would be improved service, operational cost reductions. Long-term, replacing commercial communications subscriptions currently under contract with AT&T and Cox would save approximately $375,000 per year, resulting in a payback period of more than four decades. With an installed fiber network, there may be second order revenue opportunities through leasing available conduit to telecommunications companies, utilities, and other private entities. Private companies, especially telecommunications companies, may be interested in leasing dark fiber. There may also be partnership opportunities with community anchors and business parks.

Next, Magellan addresses how the proposed network will address the core seven design principles outlined by the City: Scalability, Performance, Interoperability, Multi-use, Reliability, Security, and Operations.

Finally, Magellan suggests that consideration be given to issuing an RFP for alternative fiber network solutions, instead of direct fiber network construction, as costs of construction may be too great.

1.3.2 Data Center

This section provides an assessment of whether the City's current data center offers adequate protection for basic services and can support additional capacity for supporting the implementation of the latest smart city technologies served by a multi-gigabit fiber and wireless network including, VoIP, interactive kiosks, HD cameras, smart streetlight controllers, intelligent transportation devices, sensors and many other IP enabled devices and applications. The Plan then enumerates a series of controls that should be implemented, with annual reviews recommended. Each control is named; provides a statement of the control's objective; a risk statement in the event the control is not implemented; and a value statement regarding the control. (Detailed templates are provided in Appendix B for each of the controls. The templates list a minimum set of data and City should define the values and processes around each.)

Recommended controls include the following:

- Environmental Controls
- Physical Security Controls
- Secure Workspace Program
- Secure Workspace Perimeter
- Secure Workspace Access Reporting
- Secure Workspace Compliance Inspections
- Visitor Management
- Business Resiliency
- Business Impact Analysis
- Risk Assessment
- Business Activity Level Recovery Planning
- Backup Media Creation and Restoration
- Disaster Recovery, Business Continuity Testing
- Business Insurance
- Infection Disease Planning

1.3.3 Telephony

This section provides an overview of voice-over-IP ("VOIP") telephony, including definition of available functions, a comparison of on-premise vs cloud hosted advantages and disadvantages along with relative costs, preliminary cost estimates. From an infrastructure perspective, City has upgraded its switches to power-over-Ethernet ("POE"), easing transition to VOIP which will require only VOIP handsets.

As VOIP application may run either on premises at the City data center or as a service (in the cloud), the Plan compares the two solution paths.

First, Magellan summarizes the pros and cons of the VOIP application running as a service (in the cloud) comparing with the application running on premises. Magellan then provides a table of comparative costs.

Rough cost estimates for a cloud-hosted solution include:

- $10 per month per user or $15,000 per month for 1,500 phones ($180,000 annually)
- Limited staffing
- Monthly SIP trunk costs
- All costs are operating expenses

Cost estimates for an on-premise solution include:

- $300,000 for new phones
- $55,000 new server, gateways, firewalls and software
- 2 FTE staff ($250,000 annually)
- Ongoing upgrades maintenance agreements - $5,000- $7,000 annually
- Training
- Monthly SIP trunk costs
- All costs are likely operating expenses, including phones (due to low unit costs)

Finally, Magellan recommends that City issue a Request for Proposals ("RFP") to identify a Citywide VOIP solution for acquisition and implementation.

1.3.4 Video

This section provides an overview of video and its uses in cameras for the purposes of security monitoring, for traffic monitoring, and ultimately planning for 5G video attachments to streetlights. Included is a recommendation for a governance framework for federated operations with other entities.

Specific recommended next steps include:

- Develop phased implementation plans for new, upgraded cameras, led by ITS.
- Coordinate camera deployment with other technology upgrades.
- Identify network requirements for camera backhaul and signal aggregation points.
- Establish policies for aggregating, monitoring, retrieving, storing and sharing video content.
- Ensure network infrastructure provides direct, wired access to cameras.
- Reach out to stakeholders to establish federated video sharing agreements. Stakeholders may include County agencies located and operating within the City, Chula Vista schools, CalTrans and other mass transit entities, and large businesses.
  - Stakeholders may include neighboring cities of San Diego, National City, San Diego County, and San Diego Association of Governments (SANDAG), the regional planning entity.
- Develop systems for securely accessing video feeds and delivering video to remote users. Include chain of custody considerations.
- Develop storage, retention and archiving strategy and policy for all videos.

1.3.5 Signage and Kiosks

This section provides an overview of the purposes of signage and kiosks, which are essentially computer displays that inform citizens and visitors about activities, status, traffic and pedestrian detours, emergency situations, and other urgent or timely information. Some signage is interactive with the use of touchscreens or other means of collecting user input. Next steps include recommendations for analysis, to ensure appropriate use, decide on proper locations, etc.

Specific recommended next steps include:

- Plan for motorist-targeted displays in commercial districts and densely populated areas.
- Decide whether kiosks should additionally be used to deliver public Wi-Fi.
- Review funding for infrastructure that may be used to connect displays and kiosks.
- Determine variability, criticality and level of control for each class of displays and kiosks.
- Establish a comprehensive set of standards.

1.3.6 Sensor Networks

This section offers a brief primer on sensor technologies, and their uses. In the Plan, sensors are devices that convert energy (light, movement, pressure, etc.) to digital data on which decisions may be made or actions taken. Sensors can be as simple as automated door openers, to smart meters that measure utility flow (water, electricity), to more complex items such as traffic or pedestrian flow and parking availability. Next steps include more detailed specifications of priorities and service needs prior to detailed implementation planning.

Specific recommended next steps include:

- Determine monitoring requirements based on municipal goals and departmental activities and initiatives.
- Develop City policies for sensors, both for operation and for valid data collection and usage.
- Conceptualize full build out of sensor network and derive operational requirements.
- Prioritize build out based on strategic goals and imperatives.

1.3.7 Wi-Fi and Municipal Wireless Systems

This section merges two proposal tasks. In it, Magellan analyzes and evaluates municipal wireless infrastructure systems which are private and secure, and which can provide the basis for Citywide municipal Wi-Fi, if desired. Discussions of technology standards, the differences between Wi-Fi and mobile wireless and transitions to 5G technologies are included. There should be both secure, authenticated Wi-Fi for use by City employees, staff and contractors; public access Wi-Fi at City locations, for use by the visiting general public; and long-term, possibly Citywide municipal Wi-Fi. As of Dec 2019, City manages 120-130 Wi-Fi access points.

Specific recommended next steps include:

- Identify objectives, scope and purposes of citywide wireless network covering all City government buildings. These could include consolidating the several Wi-Fi networks into a single, unified network; providing greater coverage; resolving gaps in network coverage; supporting use of other devices, including tablets, 5G devices, digital signage, kiosks, sensors,; support for recreation centers and parks, event spaces, and temporary gathering spaces; providing ubiquitous Wi-Fi, etc.
- Examine and assess possible business models to determine sources of funds for capital investment and support of ongoing operation. This could include several options including: public ownership and operation, public ownership with contracted operation, public-private partnerships, or hybrid models combining traits of multiple options. Risk assessment should be included, assessing financial, operational, and business interruption risks.
- Beyond public Wi-Fi, analyze how Wi-Fi might be used for enhanced public safety applications, transit and transportation applications, field access for code enforcement and inspections, congestion management, etc.

1.3.8 Operations and Maintenance Costs

This section focuses on the ITS department, its current project lists, and absolute minimal additional staffing required to enable the ITS organization to provide support for Smart Cities initiatives. As of 2019, ITS had thirteen (13) staff under the leadership of IT Director Ed Chew. In addition, three (3) staff are detailed to Police Department with a dotted-line reporting responsibility back to Mr. Chew, to ensure consistent direction of infrastructure that is utilized throughout the City.

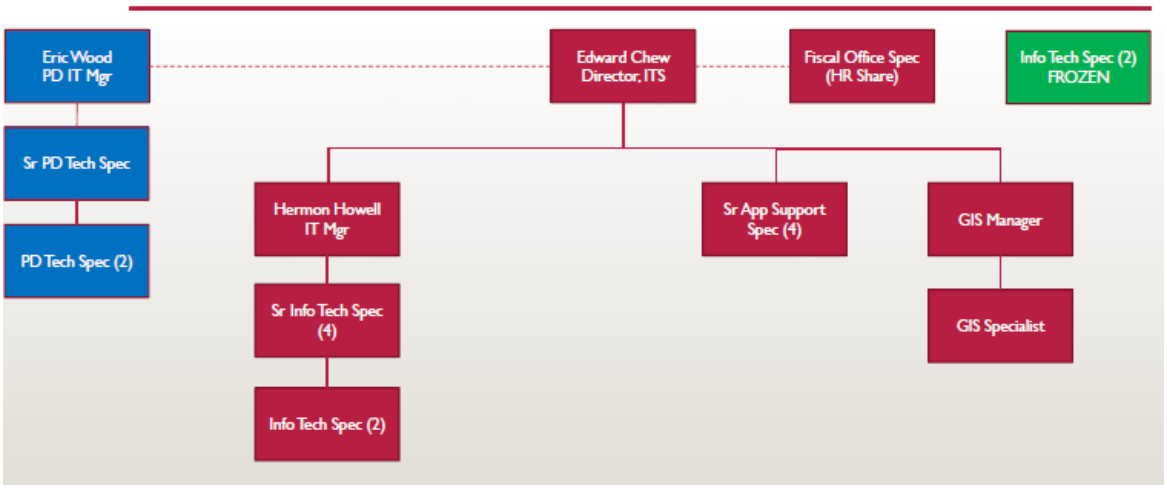


Figure 1-6 Information and Technology Services Organizational Chart

As of November 2019, there are at least twenty (20) significant projects on the ITS projects list, many of which focus on operational improvements and security, and not strategic initiatives. The projects list is included in this section.

Magellan recognizes that budgets are limited in Chula Vista. Magellan also realizes there are many years of work in the above project list. However, Magellan recommends the addition of one (1) Senior Engineer ($150-170K) and one (1) Senior IT Specialist ($135-$150K) to work on project backlog and support design of Smart City initiatives. Project Management improvements are necessary, to increase project capacity, standardize project execution, and provide consistent status reporting to senior management; Magellan recommends one (1) Project Manager ($140-160K). Finally, with cyber-security concerns ever-present and increasing, Magellan recommends creation of a Chief Information Security Officer ("CISO") role ($150-$175K). (All position estimates are fully loaded, including 30% benefits.)

1.3.9 Current Environment (Suitability for Smart Cities)

This section outlines the minimum City requirements for supporting Smart Cities initiatives. The four identified necessities are:

- Citywide fiber network – Must be robust enough to provide backhaul for 5G and other smart devices strategically placed throughout the City. The fiber network may be newly constructed or leased from commercial providers or other partners.
- Policies to support data and usage – With large amounts of data being captured and published to support Smart City initiatives, the policies required for governing data, use and protection of data must be defined and approved.

- Appropriate pricing – City has many valuable assets, including streetlights and other vertical assets. Consistent, legitimate and valid pricing must be developed to support timely responses to licensing applications, and to monetize City assets where possible.
- Necessary additional staffing – ITS staffing today is insufficient to support its backlog of projects. Significant, or even several, Smart City initiatives cannot be reliably or timely supported with current staffing and budget. Staffing augmentation contracts and contractors may provide specific technical skills but will require additional funding.

Magellan also included a SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis of the ITS organization. (ITS is the primary supplier of internal technology services within the City.)

1.3.10 Data Policies

This section identifies the considerations for five data policies: Data Privacy; Open Data; Data Ownership; Smart Cities Readiness; and Dig Once. These are prototype policies and need to be reviewed internally with key City departments, to flesh out details. Once in finished form (not in scope to this report), these should proceed to reviews and approvals by City Management and, if necessary, City Council. Each policy should be finalized and standalone. (Some identical terms are defined in several policy examples.)

- Data Privacy Policy - provides a framework for protecting personal information collected by the City and sets the boundaries for appropriate use. In finalizing the policy, many classes of data must be defined and each may have its own limits.
- Open Data Policy - provides a framework for defining how specific data sets might be made available to the public via a portal, a website, etc. both protecting the City while not compromising the identity or rights of the provider or subject of the data.
- Data Ownership Policy - provides a framework for proper use, storage and management of data across all City agencies and departments. The Policy should outline expectation of data access, availability, and management to ensure cross functional decision making while preserving data integrity and accountability.
- Smart Cities Readiness Policy - provides the framework for City to set policy to enable the implementation and support of Smart Cities initiatives. The final policy should include the desired outcomes, limits on possible partnerships, and set limits and permissions on the use of data required to support the initiative.
- Dig Once Policy - frames the policy over minimizing the cost, disruption, and frequency of placement of road, utility, and other infrastructure. The final policy should include considerations of joint trenching, which encourages communications between and among City agencies and departments, and with external parties such as utilities, to ensure, wherever possible, that conduit, and possibly fiber, are placed whenever infrastructure is opened for work. This policy may include guidance on moratoria, and cite valid exceptions, such as for emergency repair. (A complete Dig Once policy is included as Appendix A.)

1.3.11 Wireless Systems Security

This section provides guidance on securing systems which are collecting ever-increasing amounts of wireless data, all of which require appropriate security and handling. These systems include municipal and City employee applications, public safety applications, public use applications, and wireless hotspots.

Specific analysis for security considerations and assessment of the following areas is provided:

- Outdoor Wireless Network Applications, including City applications; Public Safety applications; and Public Use applications, which are targeted at residents, businesses, and tourists. Outdoor wireless deployment architecture, hotspots, hot zones and roaming considerations across multiple subnets is discussed.
- Fiber backhaul and other transport considerations are assessed.
- Other security considerations on next generation communications platforms, including Wi-Fi 5, Wi-Fi 6, and the general IEEE 802.11 standard are discussed.

1.3.12 Governance

Recommendations for expansion of the IT oversight program includes broadening the scope of program and project review to include prioritization, spending estimates, and strategic positioning.

Recommendations on improved project management focus on establishment of project management guidelines and the establishment of a Project Management Office ("PMO"). The PMO would leverage the Project Management Book of Knowledge ("PMBOK") to define processes and templates acceptable to the City.

Finally, Magellan recommends that the policy development process be documented.

1.3.13 Valuation of Key Assets

This section provides a valuation analysis for 5G wireless pole attachments which may be affixed to streetlights and other City assets. It discusses FCC's Wireless Order, 18-133, which is currently in effect but under appeal in Ninth Circuit Court. The analysis discusses the timeline shot-clock for reviews and approvals of permit applications which might be submitted by wireless carriers, the framework for aesthetic guidelines which City may require, and the fees cities may reasonably charge for permits and annual attachment fees. FCC's safe harbor annual fee of $270 per pole per year is discussed.

1.4 IN CONCLUSION

The City of Chula Vista is actively planning its long-term Smart Cities vision. This Telecommunications Master Plan, with its primary focus on creation of a citywide fiber network and recommendations for complementary technologies, policies and processes, helps position the City to move forward to provide new services, technologies, and applications. These will

support faster growth and economic development, permitting Chula Vista to continue its growth and increase prosperity.

2. Core Infrastructure and LAN/MAN Opportunities

Magellan Advisors has combined Core Infrastructure (proposal task 1) and LAN/MAN (proposal task 3) as both tasks are inextricably linked in their background information and current situation. As a result, it is prudent to combine both tasks into a single set of recommendations to maintain the continuity of the goals and narrative surrounding an integrated fiber optic network infrastructure and to construct a single unified plan for improving and upgrading. With that, the following section takes a comprehensive view of Chula Vista's current networks, strategic departmental initiatives, desired integration strategy, and opportunities for operational improvement.

2.1 BACKGROUND

The City of Chula Vista currently has three different departments managing various aspects of enterprise information technology ("IT"), including City IT, Traffic Operations, and the Police Department. Each department develops its IT strategy independent of the others, with a focus on departmental application needs and operations within their respective functional areas, but each is anticipating and expecting a common IT infrastructure on which their applications will run.

A fiber cut could result in a complete service outage to connected buildings with the current network architecture.

City IT is located in the City Hall complex, and is responsible for the overall network citywide, data and voice services, and internet access. City IT is also responsible for virtualization, and storage infrastructure (except for Police which handles these services and its own applications and other services). The network infrastructure is primarily comprised of traditional leased telecommunication services from Cox and AT&T. Some limited fiber is used to connect the city hall data center in Civic Center C to the following buildings:

- Traffic Management Center in Civic Center B at 276 4th Avenue
- Police Department at 315 4th Avenue
- Fire Station 1 at 447 F Street
- Civic Library at 365 F Street
- South Library at 389 Orange Avenue

This fiber exists in point-to-point lateral routes without diverse path protection.

City IT also maintains a master purchasing contract with Dell for virtualization, support services and storage equipment, which is leveraged by all three departments for support of their applications. Police Department manages its own purchases separately, however, including acquisition and maintenance of all PCs, servers, and storage.

City IT commissioned and adopted a Network Assessment Report produced by NIC Partners in April 2017. The report provided guidance in three critical areas:

- Identified obsolete hardware, security risks, and infrastructure gaps.
- Recommended specific Cisco replacement hardware and management solutions.
- Described a layer 2 / layer 3 architecture to achieve a robust, integrated network.

The NIC report did not address in detail deficiencies in, or recommendations to improve, the City's communications infrastructure.

Traffic Engineering is also located in the City Hall complex and is responsible for the Traffic Management Center. The traffic network includes a small data center with independent network infrastructure connecting 305 traffic controllers serving 267 traffic signals to the Traffic Signal Communications Center ("TSCC"). Traffic Engineering completed a Traffic Signal Communications Master Plan in July 2017 which documented significant infrastructure communication deficiencies and recommended strategies to modernize their infrastructure to a fiber-based Ethernet network. The report focused solely on the needs of the department and did not address network infrastructure replacement from a strategic integrated asset perspective, including an underlying IT communications infrastructure.

The Police Department is responsible for operations of and access to Federal and California Law Enforcement Telecommunications System ("CLETS") systems for law enforcement functions. CLETS also provides access to Federal systems, such as the FBI's Criminal Justice Information Systems ("CJIS"). Police Department is also responsible for managing all Verizon mobile services for fleet connectivity to the network. They maintain the department-specific applications that support these functions in conjunction with IT staff that are permanently located within the main police headquarters building.

2.2 CURRENT SITUATION

City IT is currently in the process of implementing recommendations from the NIC Partners report, and in fact have made significant headway in their remediation and improvement efforts. The recommendations included replacing obsolete equipment, implementing power-over-Ethernet ("POE") switches for a future VoIP conversion, enhancing the Layer 2/3 architecture for improved performance and reliability, and standardizing on Cisco's Digital Network Architecture ("DNA") to incorporate software defined networking ("SDN") capabilities and provide centralized, integrated management and security of all Chula Vista networks. To build on the previous assessment work and remediation and improvement efforts of City IT, this Telecommunications Master Plan assumes certain aspects and recommendations of the NIC Partners report. City IT is deploying a modified version of the NIC report's hardware bill of materials ("BoM") (an enumeration of all planned equipment) and network architecture, so limited documentation of the new network was available for use in this TMP. Therefore, the assumptions made in the following recommendations may differ somewhat from the actual hardware and architecture deployed.

Traffic Engineering is currently working to construct a fiber network connecting traffic controllers along major roads and replace/upgrade equipment in sections of its operational system per the TSCMP. This TMP assumes certain aspects and recommendations of that plan in order to build on the previous assessment work and recommendations. Currently, only 24 of the 267 traffic signals are connected to fiber facilities. The remaining traffic signals are connected by cellular/wireless infrastructure, or by aging copper twisted wire pair ("TWP") or are off-line entirely. The leased copper infrastructure includes 91 plain old telephone service ("POTS") and copper circuits costing approximately $75,000 annually. Section 4 of the TSCMP recommended the future traffic network infrastructure be converted to fiber as much as possible, using standard IP/Ethernet technologies for signal control, appropriate surveillance, and to support the Internet of Things ("IoT"). In addition, the TSCMP recommended establishing a second TMSS/TMC for service redundancy and/or disaster recovery which would require protected connectivity to the primary Traffic Management Center ("TMC"). Table 2-1 (below) of this report details the types and quantities of infrastructure and communication deficiencies observed in the assessment.

Table 2-1 Traffic Signal Communications Infrastructure and Deficiencies Summary from TMP

Number	DESCRIPTION	QUANTITY
-	City of Chula Vista Total	267
1	Analog Fiber Optic Communication	24
2	Serial Wireless Radio Communication	4
3	Leased Copper-Based Communication	102
4	City-Owned Infrastructure on Leased Copper-Based Communication	124
5	No Communication Due to Infrastructure Gap	11
6	No Communication Due to Leased Infrastructure Repair	2
7	Analog Video Detection	155
8	Lack of Remote CCTV Monitoring	267
9	Lack of Limited Service and/or Post-Preemption Sequence	5
10	IR-Based Emergency Vehicle Preemption	267
11	Leased Cellular-Based Communications	46*
12	Type 170 Controllers	255
13	Lack of Stand-Alone Battery Back-Up	267

*Traffic Measurement Devices are located nearby signalized intersections

The individual assessment reports are excellent resources in their context, and the department managers strive to coordinate on projects as much as possible. However, the lack of an integrated network infrastructure with centralized management and security naturally limits the degree to which technology can be effectively leveraged and limited capital can be optimized for multi-department IT operations. Duplicated effort and cost are unavoidable in non-integrated IT environments, resulting in adverse effects on network scalability, performance, interoperability, multi-use facilities, reliability, security, and operations in several ways.

A network's scalability is the property of being easily expanded or upgraded on demand to meet the changing requirements of applications, technology, and growth. The current network depends on services from Cox and AT&T, which severely limits scalability of service types and bandwidths to what is offered by these third-party incumbents. In addition, City IT and Traffic Engineering operate separate data networks for application and traffic signal control, thereby limiting scalability of network connectivity, maintenance, security, and management. A single citywide fiber network, managed by ITS and appropriately secured with firewalls and anti-virus and -malware infrastructure, would ensure the integrity of operation for the network, while not constraining the flexibility required for the Police Department and Traffic to implement their own applications. Virtual private networks between internal groups and external entities, can simply be transported over the City's fiber network.

A network's performance is a measurement of its ability to make information available in the form, timeliness, and accuracy dictated by its design and required by its end users. Objective performance can be measured using element managers such as Cisco's Evolved Programmable Network Manager ("EPNM") and third-party tools such as Wireshark and Metageek Chanalyzer. Subjective performance is typically determined by its end users and is a perception of the network's ability to meet their IT-related needs in real time. End-to-end performance management of the City's networks is currently constrained by factors such as obsolete telecom services, variation in circuit types, differences in hardware and software configuration, and the types of end point devices.

A network's interoperability defines the extent to which it can connect to, function with, and manage/be managed by separate networks and equipment. The City's separate networks are not presently connected or configured in a way that allows City IT to manage and monitor the infrastructure as a single integrated system. In addition, City ITS should arrange for additional service contracts to either provide security training for existing and additional staff, or secure security services from a third-party provider. Software-defined networks product provides a fabric for software-defined networks, including the framework of properly security all high-end telecommunications equipment, offered by Cisco, among others. Cisco Advanced Services provides these configuration services.

Multi-use facilities refer to a network's capability to leverage common assets for operations and maintenance. While the City has been working toward consolidating data centers, virtualization, and storage infrastructure, its core infrastructure can be improved. For example, by defining virtual private networks, Police could connect to CLETS to permit secure, reliable connections to mandated services in support of public safety, while still providing City with a central fiber infrastructure and ITS-supported management. In addition, upgrades to firewalls are likely required

Reliability refers to the dependability of a system to be available for use when required. The reliability of a network is determined by its architecture, equipment configurations, and

operational practices. While the City's leased network services are generally reliable, City IT has indicated the existing fiber connecting critical facilities is not redundant, and therefore unable to survive a cut or optical interface failure. In addition, the older analog "plain old telephone service" lines and wireless technologies used in Traffic Engineering's infrastructure are not as reliable as the new fiber and Ethernet infrastructure platform to which they are migrating.

Security of a network infrastructure is critical physically, logically, and operationally. The physical location of hardware and telecommunications facilities can compromise the integrity of components through either intentional or unintentional means. The logical configuration of hardware, servers, and firewall systems can compromise the integrity of their operations through both user error and malicious third parties. The operational practices of an organization can compromise the best physical and logical security through negligence or deceit. Security management, when distributed across departments on an integrated infrastructure, can result in unintended access and control gaps through configuration and/or operational mismatches. The City holds network security in high regard as evidenced by its efforts to upgrade and replace network infrastructure and equipment.

The operations of a network involve the day to day functions of staff and contractors to maintain the network's usability, performance, reliability, security, and regulatory/legal compliance. Sufficient staff and skillsets are required to maintain an acceptable level of operational performance. City IT currently maintains a staff of ten (10), including six (6) within the IT department, three (3) within the Police Department, and an IT department director. These staffing numbers are insufficient to support the planned technology upgrade plan proposed in this TMP, and are insufficient for supporting demand for enhancements to today's operations. Due to excessive demands on ITS staff, execution plans for new strategic initiatives such as Smart Cities, there is insufficient time for comprehensive planning for these efforts. Staffing will be further addressed in Operations and Maintenance Costs, Section 9 of this Plan.

2.3 SITE CLASSIFICATION

Construction of new fiber requires significant capital investment but gives the City ownership of the network, and more important, long-term control and financial certainty of communications costs.

The City should invest capital dollars to build a fiber network and budget annually to operate it, thereby permanently eliminating the recurring costs associated with procuring leased network services. The City would own the critical digital infrastructure required to comprehensively serve its IT needs for the foreseeable future. Additionally, the City will be able to scale the network to support future initiatives such as the Smart Bayfront project and Smart City applications as part of Strategic Action Plan at incremental capital costs, versus endlessly increasing operating costs by growing monthly recurring leased services. A fiber network will also improve the City's public safety standing in several ways:

- Shifts financial and operational control of the network infrastructure to the City
- Reduces reliance on third-party operators
- Hardens critical infrastructure – by providing a single secure and managed fiber infrastructure

In addition, the proposed phased fiber construction fully supports the objectives set forth in Sections 1.5, 4, and 5.5 of the Chula Vista Traffic Signal Communications Master Plan.

The network should be constructed in six (6) largely independent phases, consisting of three backbone rings, City sites, and traffic control systems. Of the six phases, the first three are the most crucial to accomplishing the goals set forth by Chula Vista for this project and the recommendations made in this Plan. Table 2-2, below, displays each of these six phases.

Table 2-2 Network Construction Phases

Phase	Recommendation	Phase Scope, Description
1	Required	Backbone Ring 1, Connecting Data Centers and Aggregation Sites
2	Required	Traffic Network Connecting to Ring 1
3	Required	Laterals Connecting City Sites to Ring 1
4	Contingent	Backbone Ring 2 and Laterals to City Sites
5	Contingent	Traffic Network Connecting to Ring 2
6	Contingent	Backbone Ring 3 (Blue) and Remaining Traffic Network

Implementation of the second and third rings are contingent on availability of complete funding for a phase.

Phase 1 creates a physical ring consisting of 288-count fiber diversely routed to connect City IT, the Police Department headquarters, Traffic Management Center, and Public Works. This physical ring connects to core switches at each site to provide both protected high-speed transport among the data centers and remote site aggregation for end user access to the applications and storage. In addition to remote City sites, the ring also aggregates the traffic control networks, surveillance systems, and future Smart City components.

Phase 2 follows the Traffic Signal Communications Master Plan to construct fiber for the traffic networks in downtown Chula Vista. The traffic networks could be deployed in physical rings or daisy chained configurations depending on available equipment budget and fiber topology. Each group of signal controllers terminates to the aggregation switches on the transport ring for connectivity to the primary Traffic Management Center.

Phase 3 constructs fiber to connect sixteen (16) of the twenty-seven (27) City sites, including Civic Center C, using 24-count laterals from each site to the aggregation switches on the transport ring.

This would migrate most City sites to City-owned fiber and allow the disconnection of monthly recurring leased services to those sites. (For purposes of analysis, Magellan mapped 42 parks and recreation centers, and 42 communications towers. For budget minimization. Magellan is not recommending connecting all parks.)

Phase 4 constructs a second physical fiber ring connecting sites and traffic networks in the northern half of the City. This ring would be used to aggregate city sites and traffic networks to the primary ring for termination into one or more of the aggregation sites. In addition, 24-count laterals would be constructed to the remaining seven remote City sites.

Phase 5 constructs the networks serving the northern traffic signals and terminates them to the aggregation sites on the primary ring for connectivity to the Traffic Management Center.

Phase 6 constructs a third physical ring connecting the southern half of the City, providing future fiber connectivity as growth occurs. The remaining traffic networks would also be transported by this ring to the aggregation sites for connectivity to the Traffic Management Center.

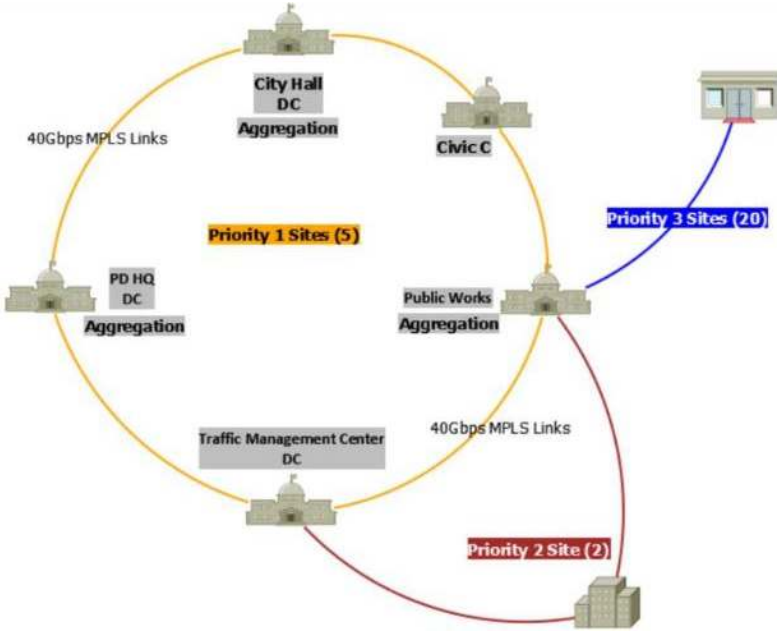


Figure 2-1 Chula Vista Conceptual Network Architecture

The fiber engineering will be designed to distribute termination of all remote endpoints across three aggregation sites located in the City Hall complex, the Police Station, and the Public Works facility. The remote sites and traffic networks will be migrated off their existing managed services to the new fiber network over the course of each construction phase. Existing customer premise equipment ("CPE") will be re-used by replacing copper network interfaces with small form-factor

pluggable optics where possible, with site cutover coordinated during phases 3 and 4. Non-fiber capable signal control equipment that is targeted for replacement would be procured and coordinated for replacement during phases 2, 5, and 6. City IT staff will coordinate the cutover of the sites with each department's local staff. City IT will need to work with NIC Partners to assess their existing edge switch network interface types and identify changes required to accommodate single mode fiber connections.

A substantial benefit of constructing a ring-based fiber infrastructure is improving the reliability of the City's network. Once connected to the ring, there would be two paths to internet points of presence, traversing in either direction. There is still the risk of service loss in the event of a cable cut into the building Currently, the City data centers, remote sites, and signal control networks are connected on unprotected leased circuits and fiber laterals. Today, in the event of a cable cut or equipment failure, the affected site(s) will experience a complete service outage until the failure is corrected. Such an outage at one of the data centers would result in extended outages for multiple remote City sites or signal controllers terminating in it. This would likely result in material impacts to City operations, and to Chula Vista citizens if critical applications are affected.

To mitigate this possibility, in consultation with Magellan, City staff has assigned a priority of 1, 2, or 3 to each City site reflecting the impact of its outage on staff and citizens. Priority 1 ("P1") sites will serve as transport nodes and/or aggregation points for remote City sites with fully diverse fiber routes and redundant equipment. P2 sites will be connected to the network using two diversely routed data services to separate P1 aggregation sites, providing redundancy; P2 sites will be configured to failover to the backup connection should a fiber cut or if equipment failure occurs. P3 sites will be connected to the network using a single data service to a single designated P1 aggregation site. In the event of a fiber cut or other disruption, traffic will be rerouted on the remaining path from any P1 site, ensuring continuity of service.

City sites proposed to be connected, their priority and planned implementation phase can be found in Table 2-3, below. (City Park and Recreation sites are not planned to be connected, due to cost considerations.)

Table 2-3 City Sites Considered for Connection, with Lateral Priority

Site Name	Street Address	Priority	Phase
Public Works (Data Center)	1800 Maxwell Rd	1	1
Civic Center Bldg A (City Hall Data Center)	276 4th Avenue	1	1
Police Department (Data Center)	315 4th Avenue	1	1
Civic Center Bldg B (Traffic Mgmt Center)	276 4th Avenue	1	1
Civic Center Bldg C	276 4th Avenue	1	3
Civic Library	365 F Street	2	3
South Library	389 Orange Avenue	2	3
Animal Control	130 Beyer Way	3	3
Boys and Girls Club of Chula Vista	1301 Oleander Av	3	3

Fire Station #3	1410 Brandywine Ave	3	3
Fire Station #9	266 E Oneida St	3	3
Chula Vista Women's Club	357 G Street	3	3
Fire Station #5	391 Oxford Street	3	3
Bonita Public Safety Center	4180 Bonita Rd	3	3
South Bay Community Services	430 F St	3	3
Fire Station #1	447 F St	3	3
Chula Vista Community Youth Center	465 L St	3	3
Chula Vista Harbor	550 Marina Pw	3	3
Visitor Information Center	750 E Street	3	3
Fire Station #2	80 East J St	3	3
Fire Station #8	1180 Woods Dr	3	4
Fire Station #7	1640 Santa Venetia St	3	4
Otay Ranch Community Storefront	2015 Birch Rd	3	4
Olympic Training Center	2800 Olympic Pkwy	3	4
Fire Station #6	605 Mount Miguel Rd	3	4
Fire Station #10 (Future)	610 Bay Blvd	3	4
Fire Station #4	850 Paseo Ranchero	3	4
Chula Vista Community Park	1060 Eastlake Pkwy	3	N/A
Breezewood Park	1091 Breezewood Drive	3	N/A
Voyager Park	1178 E J Street	3	N/A
Greg Rogers Park	1189 Oleander Av	3	N/A
Independence Park	1248 Calle Santiago	3	N/A
Rancho Del Rey Park	1311 Buena Vista Way	3	N/A
Palomar Park	1359 Park Drive	3	N/A
Santa Cora Park	1365 Santa Cora	3	N/A
Heritage Park & Recreation Center	1381 E Palomar Street	3	N/A
Sunset View Park	1390 S Greensview Drive	3	N/A
Loma Verde Aquatic Park & Rec. Center	1420 Loma Ln	3	N/A
SDG&E Park	1450 Hilltop Drive	3	N/A
Orange Park	1475 Fourth Ave	3	N/A
Mountain Hawk Park	1475 Lake Crest Drive	3	N/A
Los Ninos Park	150 Teal Street	3	N/A
Santa Venetia Park	1500 Magdalena Ave	3	N/A
Rienstra Sports Complex	1500 Max Ave	3	N/A
Montecito Park	1501 Santa Diana Road	3	N/A
Harvest Park	1550 E Palomar Street	3	N/A
Connoley Park	1559 Connoley Ave	3	N/A
Otay Park	1613 Albany Ave	3	N/A
Windingwalk Park	1675 Exploration Falls Drive	3	N/A
Tiffany Park	1713 Elmhurst Ave	3	N/A
Bonita Long Canyon Park	1745 Coltridge Lane	3	N/A
Cottonwood Park	1778 E Palomar Street	3	N/A
All Seasons Park	1825 Magdalena Avenue	3	N/A
Stylus Park	2025 Stylus Street	3	N/A

Mount San Miguel Park	2335 Paseo Veracruz	3	N/A
Norman Park / Senior Center	270 F St	3	N/A
Salt Creek Park & Recreation Center	2710 Otay Lakes Rd	3	N/A
Eucalyptus Park Ball/Sports Fields	276 4th Av & C Street	3	N/A
MacKenzie Creek Park	2775 Mackenzie Creek Rd	3	N/A
Lauderbach Park	333 Oxford Street	3	N/A
Otay Recreation Center	3554 Main Street	3	N/A
Memorial Bowl / Park	373 Park Way	3	N/A
Parkway Aquatic/Community Center	373 Park Way	3	N/A
Holiday Estates I & II Park	383 Connoley Circle	3	N/A
Gayle L. McCandliss Park	415 E J Street	3	N/A
Terra Nova Park	450 Hidden Vista Drive	3	N/A
Rohr Park	4548 Sweetwater Road	3	N/A
Friendship Park	4th Av & F Street	3	N/A
Sunbow Park	500 E Naples Street	3	N/A
Valle Lindo Park	545 Sequoia Drive	3	N/A
Harborside Park	670 Oxford Street	3	N/A
Sherwood Park	69 Sherwood Street	3	N/A
Discovery Park	700 Buena Vista Way	3	N/A
Lancerlot Park	750 K Street	3	N/A
Paseo Del Rey Park	750 Paseo Del Rey	3	N/A
Hilltop Park	780 Hilltop Drive	3	N/A
Veterans Park & Recreation Center	785 E Palomar Street	3	N/A
J St Marina Bayside Park	800 Marina Pkwy	3	N/A
Montevalle Park & Recreation Ctr.	840 Duncan Ranch Rd	3	N/A
Marisol Park	916 Rancho Del Rey Pkwy	3	N/A
Sunridge Park	952 Beechglen	3	N/A
Horizon Park	970 E Palomar Street	3	N/A
Bay Boulevard Park	F Street & Bay Blvd.	3	N/A
Explorer Park	Rancho Del Rey Pkwy & Norella St	3	N/A

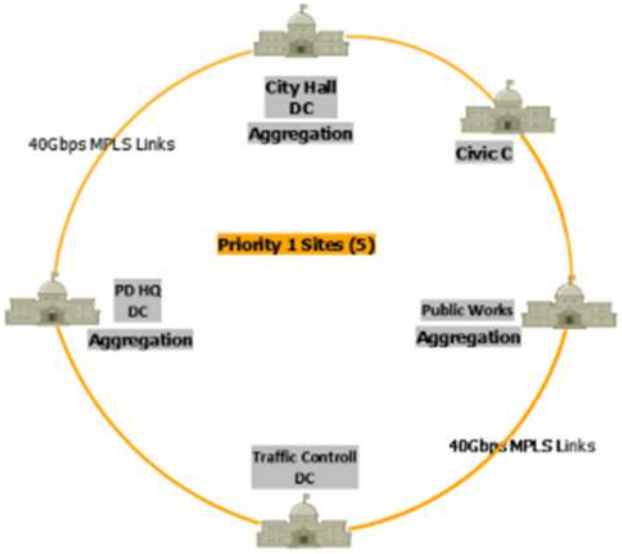


Figure 2-2 P1 Site Network Nodes

Priority 1 (P1) sites are considered primary network nodes and will be designed for maximum redundancy in both fiber cable connectivity and network equipment functionality. These sites typically sit directly on the backbone fiber ring and contain termination capacity for high-count backbone fibers and fiber distribution panels to allow both ring and lateral connections to network equipment. P1 sites consist of primary data centers, network aggregation points, collocation sites, and other high-value and/or highly available locations.

Priority 2 (P2) sites are considered redundant network sites and will be designed with two diversely routed lateral connections to separate P1 node sites to prevent a single point of failure with a cable cut or network hardware failure. In the event of such a failure, network protocols will fail traffic to the surviving link so that application and Internet service is maintained at the site. P2 sites consist of secondary data centers, critical service sites, and other locations deemed by City as critical to service and network uptime.

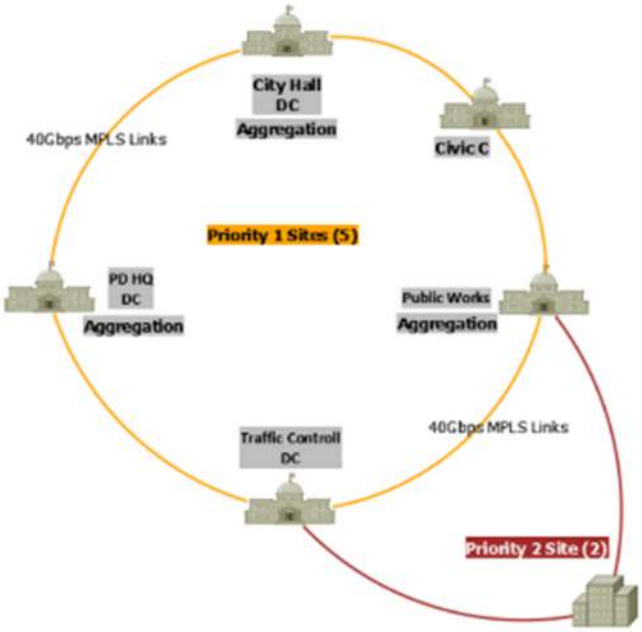


Figure 2-3 P2 Site Network Nodes

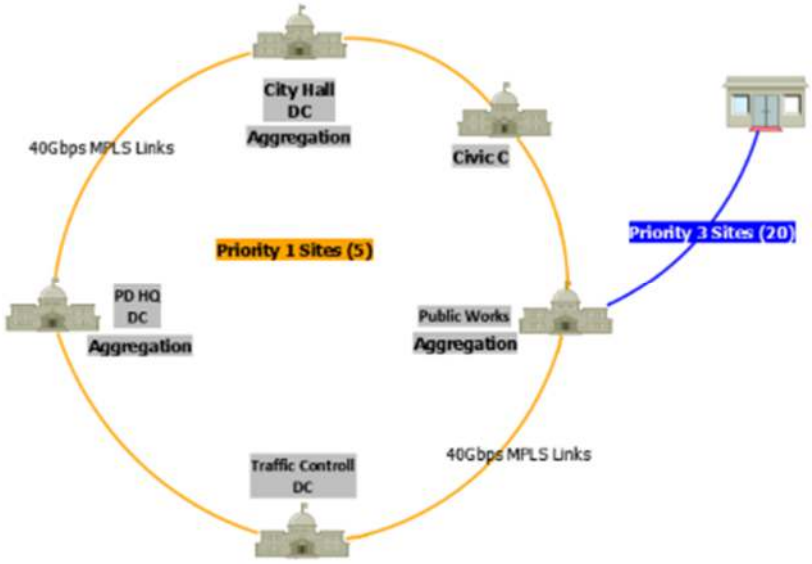


Figure 2-4 P3 Site Network Nodes

Priority 3 (P3) sites are considered non-critical to service and network uptime. They are designed with a single fiber lateral cable feeding a single pair of backbone fibers connecting the site to a single P1 aggregation site. In this configuration, a fiber cut or electronics failure at any point between the aggregation site and the P3 site would isolate the P3 site, leaving service to the site temporarily unavailable.

2.4 CONSTRUCTION PHASING

The Chula Vista backbone network will traverse 33 miles of City roadway infrastructure and conduit routes, passing City-owned buildings, traffic control systems, areas of future development, third-party networks, and other locations strategic to the City. In addition, the backbone cable may contain feeder and distribution cable for extension of network services from the nearest equipment point-of-presence ("POP") to network access points for the tie-in of connecting sites. Backbone cables will be sized in multiples of 144 fibers. The planned backbone will incorporate enough fiber capacity to meet the City's site-to-site connectivity needs, traffic signal and video monitoring system connectivity, future Smart City initiatives, as well as capacity to lease dark fiber if the City so chooses.

Lateral segments will cover 54 miles of access routes to connect twenty-seven (27) City-owned sites to the backbone fiber. Seven (7) sites, including the three data centers and a network aggregation site, will be connected by two diversely routed laterals with separate building entrances to prevent a single point of failure with a fiber cut. The remaining twenty (20) City-owned sites will be connected by a single lateral. Laterals are typically 24 fiber cables extending from a backbone splice enclosure into the building premise, terminating in a telecom equipment room for network service hand-off.

Table 2-4 (below) presents several relevant summary statistics of the proposed fiber network:

Table 2-4 Phasing Summary – Conceptual Network

Phasing Summary - City of Chula Vista Conceptual Network					
	Laterals			Backbone	
Phase	Sites Connected	Lateral Footage	Engineering, Labor, and Materials Cost	Backbone Footage	Engineering, Labor, and Materials Cost
1	4	2,539	$123,970	73,371	$2,935,995
2		112,855	$3,792,037		
3	16	35,953	$1,345,357		
4	7	31,332	$1,133,469	70,343	$2,808,433
5		81,280	$2,944,547		
6		17,971	$655,528	32,953	$1,341,064
Totals	**27**	**281,930**	**$9,994,908**	**176,667**	**$7,085,492**

(Totals may be off slightly due to rounding.)

The estimated costs above are order of magnitude costs, and include all construction labor, material, engineering, and permitting. They do not, however, include any contingency, permit fees, project management, or construction management. Estimated costs for project and construction management will depend on the length in months of each phase.

Phase 1 – Backbone Ring 1 Connecting Data Centers and Aggregation Sites

Phase 1 includes 13.9 route miles of fiber consisting of the primary backbone fiber ring and connection of four sites, including City IT, Police Headquarters, Traffic Management Center, and Public Works. All four buildings are designated as P1 sites.

Figure 2-5 Phase 1 Route Map

Phase 1

Table 2-5 Phase 1 Buildout Cost

Phase 1 - Backbone Buildout Core Ring and IT Data Centers					
Description	Ft	Labor	Material	Cost/ft	**Total**
Backbone - All New duct, handholes & cablir	73,371	$2,364,219	$480,062	$38.77	**$2,844,281**
Description	Ft	Labor	Material	Cost/ft	**Total**
Laterals to IT Data Centers sites on Core Rii	2,539	$99,906	$20,890	$47.58	**$120,796**

Phase 2 – Traffic Network Connecting to Ring 1

Phase 2 includes 21.4 route miles and connections to twenty-one (21) adjacent and nearby traffic signals.

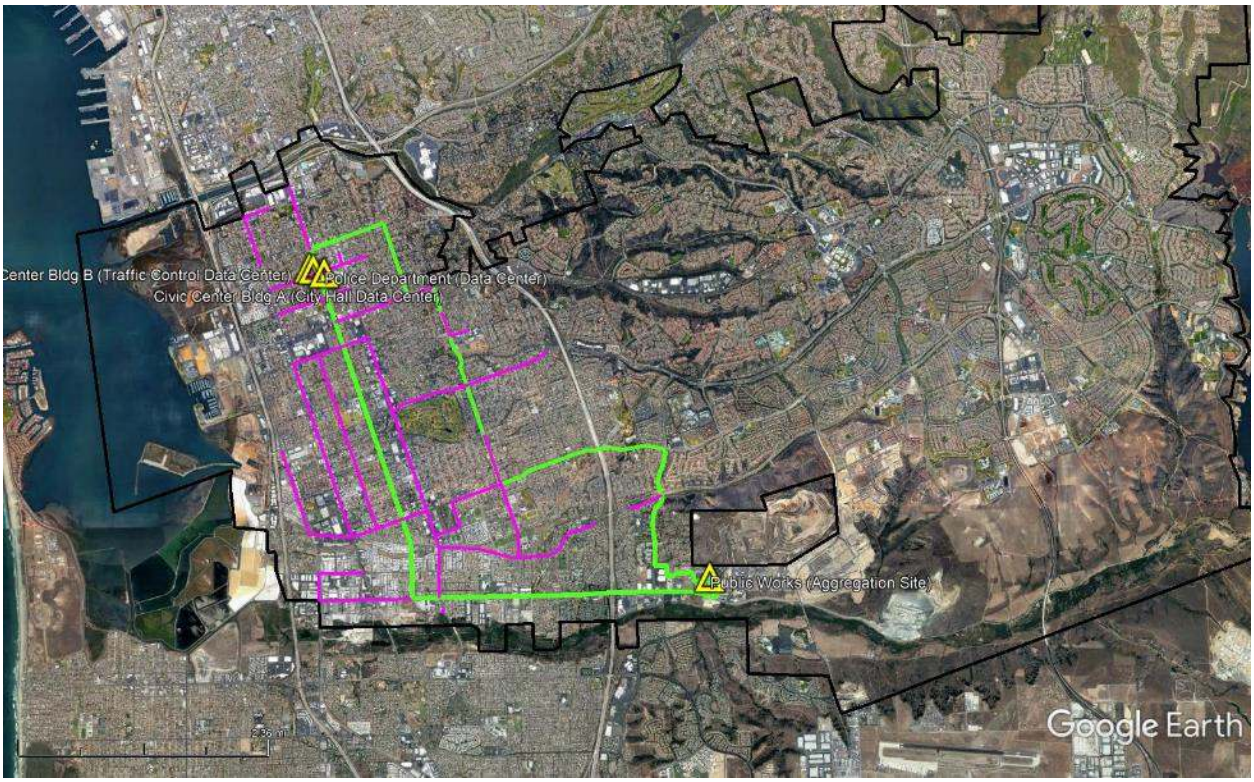


Figure 2-6 Phase 2 Route Map

Phase 1
Phase 2

Table 2-6 Phase 2 Buildout Cost

Phase 2 - Core Ring Signals					
Description	Ft	Labor	Material	Cost/ft	**Total**
Laterals to Signals on the Core Ring	112,855	$3,449,766	$201,202	$34.95	**$3,650,968**

Traffic Engineering currently has 288-count fiber installed along Fourth Avenue, and 144-count fiber along three (3) other routes. This existing fiber may be re-configured to offset some of the proposed construction for Phases 1 through 3. The affected footage is unknown and this data must be collected. This data collection effort will require OTDR tracing or other documentation unavailable for this report.

Table 2-7 Phase 2 Routes

Route	Street	End Points
1	Fourth Avenue	Brisbane St. to Main St.
2	Main Street	Fourth to Broadway
3	Davidson Street	Fourth Ave to Guava Ave
4	H Street	Hidden Vista Dr to Fourth Ave

Phase 3 – Laterals Connecting City Sites to Ring 1

Phase 3 includes 6.8 route miles of fiber connecting sixteen (16) City sites including the Civic Library, the South Library, and five fire stations.

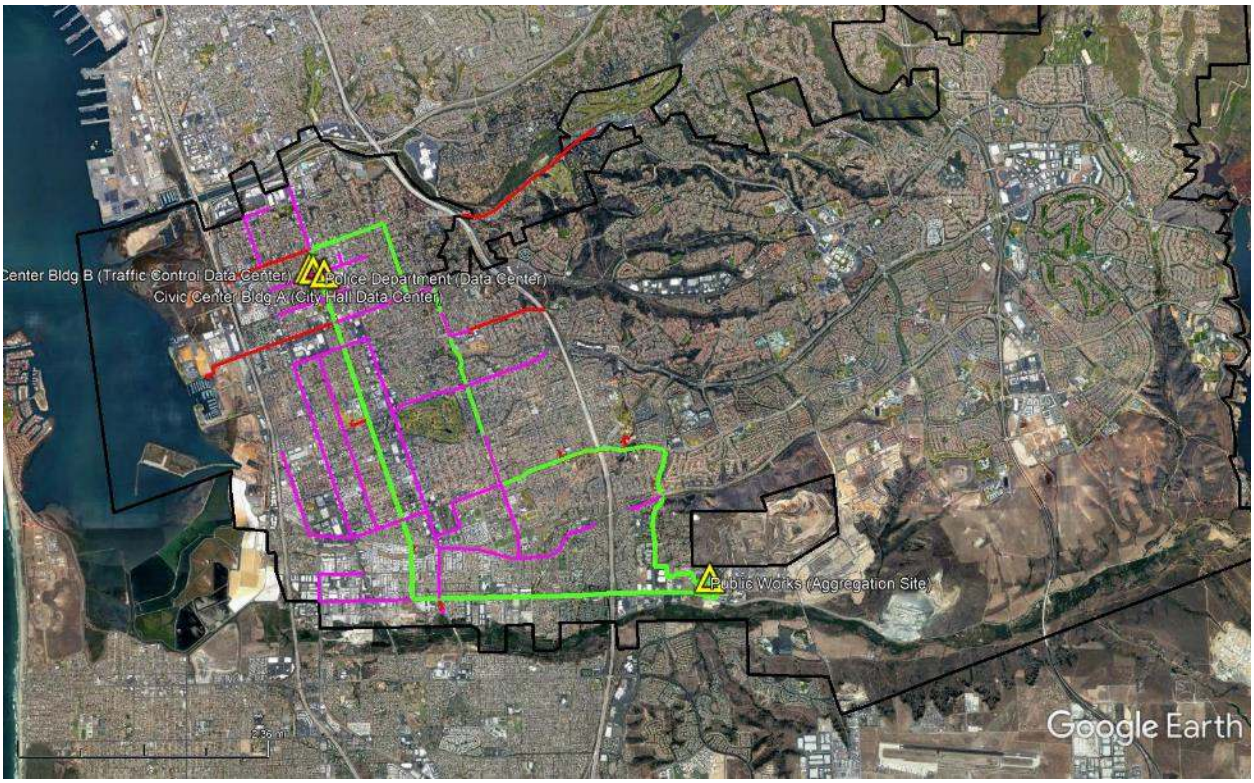


Figure 2-7 Phase 3 Route Map

Phase 1
Phase 2
Phase 3

Table 2-8 Phase 3 Buildout Cost

Phase 3 - Core Ring City Sites					
Description	Ft	Labor	Material	Cost/ft	**Total**
Laterals to key City Sites on Core Ring	35,953	$1,129,494	$170,922	$36.17	**$1,300,416**

Phase 4 – Backbone Ring 2 and Laterals to City Sites

Phase 4 includes 25.9 route miles of fiber consisting of the northern fiber backbone ring and connection of seven sites including five (5) fire stations.

Figure 2-8 Phase 4 Route Map

Phase 4

Table 2-9 Phase 4 Buildout Cost

Phase 4 - Backbone Buildout Ring 2 and Ring 2 City Sites					
Description	Ft	Labor	Material	Cost/ft	**Total**
Backbone - All New duct, handholes & cablir	70,343	$2,262,731	$457,774	$38.67	**$2,720,505**
Description	Ft	Labor	Material	Cost/ft	**Total**
Laterals to key City Sites on Ring 2	31,332	$957,219	$137,085	$34.93	**$1,094,304**

Phase 5 – Traffic Network Connecting to Ring 2

Phase 5 includes 15.4 route miles of fiber consisting of the traffic signals connected to the northern fiber ring.

Figure 2-9 Phase 5 Route Map

Phase 4
Phase 5

Table 2-10 Phase 5 Buildout Cost

Phase 5 - Ring 2 Signals					
Description	Ft	Labor	Material	Cost/ft	**Total**
Laterals to Signals on Ring 2	81,280	$2,486,062	$356,885	$34.98	**$2,842,947**

Phase 6 – Backbone Ring 3 (Blue) and Remaining Traffic Network

Phase 6 includes 9.7 route miles of fiber consisting of the southern fiber backbone ring and connections to traffic signals.

Figure 2-10 Phase 6 Route Map

Table 2-11 Phase 6 Buildout Costs

Phase 6 - Backbone Buildout Ring 3 and Ring 3 Signals					
Description	Ft	Labor	Material	Cost/ft	**Total**
Backbone - All New duct, handholes & cablir	32,953	$1,075,578	$224,295	$39.45	**$1,299,873**
Description	Ft	Labor	Material	Cost/ft	**Total**
Lateral to Signals on Ring 3	17,971	$552,790	$80,274	$35.23	**$633,065**

Phase 6 backbone can be deferred until further development of the southeastern quadrant of the City takes place, as there is no immediate driver to construct this route otherwise. The Phase 6 signal control laterals can be moved to Phase 5 if necessary, to compete the traffic network conversion.

Action Item 1: Conduct Engineering Design for the Fiber Network

The City should proceed with an engineering design of the conceptual network to use as a roadmap for all future fiber construction. This design will provide a big picture roadmap for capital investment in outside plant infrastructure that will ensure a cohesive network, whether constructed in parts to support individual departmental requirements or as a comprehensive strategic project, to serve Chula Vista's IT needs for the foreseeable future. Engineering design of all six phases for the complete system is estimated to be $573,246. As an alternative, The City could conduct an engineering design for Phases 1 through 3 of the network which would include the primary backbone ring and the majority of the City sites and traffic signal controllers connecting to it. This incremental approach would provide the roadmap for near-term fiber construction while giving the City time to conduct a financial comparison of constructing the entire network to maintaining leased data services for the foreseeable future. Engineering design for phases 1 through 3 is estimated to be $220,834. While the estimates given are reliable budgetary numbers, actual engineering costs will be dependent on field surveys and permitting requirements.

Estimated Engineering Cost	
Phases 1-6	$573,246
Phases 1-3	$220,834

Action Item 2: Construct Phases 1 through 3 of the Network

Chula Vista should plan to pursue a phased, strategic telecommunications and network infrastructure by investing capital to construct an underground conduit and fiber-optic plant to serve the long-term IT needs of the City. The City would invest in capital assets over a period of six (6) phases to construct three 288-fiber backbone rings connecting 27 City sites and 286 traffic signals to a common fiber physical plant. Funding could be made available through annual capital improvement programs or through a bond issue.

Table 2-12 Estimated Engineering, Construction, Management, and Equipment Costs

Ring	Phase(s)	Sites	Labor & Material	10% Contingency	Design and Engineering	Total Const, Des & Eng	Const Mgt	Project Mgt	Equipment *	Total
1 (Req)	1,2,3	20	7,916,462	791,646	238,073	8,946,181	180,000	144,000	283,010	**9,553,191**
2 (Cont)	4,5	7	6,657,756	665,776	228,248	7,551,779	180,000	144,000	87,080	**7,962,859**
3 (Cont)	6	0	1,932,937	193,294	106,925	2,233,156	120,000	96,000	65,310	**2,514,466**
		Totals:	**16,507,154**	**1,650,715**	**573,246**	**18,731,116**	**480,000**	**384,000**	**435,400**	**20,030,516**
			* = Includes professional services for installation							
			(Req = Required; Cont = Contingent on Funding)							

Although construction of the three backbone rings must precede the remote site and traffic signals connecting to them, the six phases are operationally independent of each other. Each phase can be implemented over three to twelve months, depending on the City's financing strategy. In addition, construction of the Phase 2, 3, and 5 remote site and traffic signal connections can be extended across multiple years if necessary, by maintaining the existing leased telecom services during the term of construction.

The operational savings through disconnection of Cox and AT&T leased services will reduce the City's monthly recurring costs over the course of the project. Detailed leased service inventories and monthly recurring costs were unavailable for use in estimating total savings per phase but should be considered when developing a capital plan for the construction. More important, the City should also consider creating financial pro-forma showing the 20-year return on investment ("ROI") of a construction project relative to the continued purchase of leased services for current and future digital infrastructure needs.

In addition, Media 3 is a regional network service provider with fiber assets in Chula Vista. They have recently offered to make their fiber available to the City, presumably through fiber sharing opportunities. The City should work with Media 3 to identify fiber assets overlapping the conceptual routes presented in this Plan and consider using their dark fiber as an offset to the total cost of construction or for strategic connectivity of sites to improve overall network resiliency.

Construction and project management costs will be based on the length of time taken for each phase, which would be decided during the fiber engineering design engagement. Network equipment costs will consist of three components, including existing core/edge modifications, remaining traffic controller replacements, and additional required software licensing. Core/edge modifications will consist of adding line cards and optical interfaces to the replacement hardware for creation of the transport ring and aggregation of connections for remote city sites and traffic networks. Traffic controller replacement equipment will consist of hardened DNA-manageable switches connected in ring and/or bus topologies to the modified edge equipment, and edge switches to connect the TMC to the transport ring. Existing traffic networks on copper and wireless infrastructure will also require switch equipment to bridge their legacy networks into the new fiber infrastructure until they can be converted. Software licensing costs will consist of any upgrades to Cisco IOS technology packages required to configure the MPLS transport ring and additional DNA licensing for traffic network devices. These configurations and costs must be developed in conjunction with Traffic's design consultant by discussing the proposed network architecture and identifying the bill of materials necessary to implement it for each phase.

Following this strategy, the City should begin construction of Core Ring 1 (Phases 1 through 3) of the network at completion of the engineering design and development of financial pro-forma demonstrating the 20-year ROI from constructing the entire network. This includes the primary backbone ring and all City sites and traffic signal controllers connecting to it. This incremental approach will provide the foundation of the City's integrated infrastructure to support near-term improvements to network reliability and traffic system upgrades while considering the timing and funding for the remaining 3 phases. Construction of Phases 1 through 3 is estimated to be $8.01 million in labor and materials, including design and engineering, and 10% contingency. Project and construction management costs consist of:

- Permit fees - determined during the engineering design
- Project management - $12,000 per month

- Construction management - $15,000 per month
- Contingency - percentage of estimated costs to account for unknowns (at 10%)

These additional estimated costs will be determined during the engineering design to provide a complete picture of the total capital investment required. Equipment costs for Phase 1 through 3 should be developed through design discussions with City of Chula Vista IT, NIC Partners and Cisco.

Action Item 3: Connect Data Centers and Aggregation Sites to Primary Transport Ring

The City will utilize the fiber backbone to establish four transport sites located at City IT in Civic Center A, the Traffic Center in Civic Center B, the Police Department HQ, and the Public Works facility. Core switches will be used to deploy a 40Gbps physical ring using meshed MPLS transport links with 50ms recovery in the event of a fiber cut or component failure. This will provide reliable fault tolerance in the event of a fiber cut or optical interface failure, and scalable bandwidth on demand by allowing the use of LACP with 802.3ad LAG groups to turn-up additional 40 Gbps links as application and storage needs grow.

Each transport site should also contain one or more Cisco Catalyst 9300 edge switches in order to aggregate connections from remote City sites, traffic signal networks, video surveillance systems, and data center switches. Virtual Routing and Forwarding ("VRF") instances will be used to create separate networks for City IT applications, traffic control, video surveillance, Internet access, and network management. Open Shortest Path First ("OSPF") will be used for internal routing and BGP with default routes would be used for routing to the City's Internet providers.

The Cisco Catalyst core and edge switches located at each transport site may require the addition of line cards and/or SFP/SFP+/QSFP optics to accommodate high speed transport circuits and/or aggregate the remote City sites connected to each of them. The MPLS circuits created between the sites will maintain full mesh transport connectivity between their core switches for compute and storage redundancy, remediating the existing single points of failure and significantly increasing network reliability. The specific Cisco modifications and hardware requirements will be developed and managed in conjunction with NIC Partners and are beyond the scope of this report.

Action Item 4: Centralize Network Management and Security

City IT has deployed new Cisco equipment supporting their Digital Network Architecture platform. This platform supports software defined networking for intent-based service provisioning, service assurance using artificial intelligence ("AI") analytics, and comprehensive threat mitigation to augment appliance-based firewalls. This advanced functionality requires an integrated network comprised of hardware supporting the DNA architecture. A common fiber infrastructure with

integrated transport and access networks will allow the full capabilities of Cisco DNA to be realized in the following ways:

A. Enhanced Network Security

Consolidating security management onto the DNA platform will allow a single view into all Chula Vista networks at key locations, devices, users, and threats in real time. Policies can be established to automatically identify threats, issue multi-department alerts, and segment the network in the event of a cyber-attack.

B. Simplified Change Management

Change management is one of the leading causes of network outages, as recently demonstrated by Google engineering on June 2, 2019. A single mis-applied configuration resulted in nearly five hours of significant performance degradation and outages to their entire application suite and tenants of their Compute Engine cloud service. Cisco's Software-Defined Access (SD-Access) will allow change management to be conducted through user policies and GUI-based hardware and configuration abstraction, mitigating the need to perform individual element provisioning and command line changes. Use of SD-Access will result in improved network reliability; however, there may still be dependencies on vendors unless significant additional hiring and training is completed.

C. Efficient Capital and Resource Utilization

Software-defined networks will support multi-domain security and provisioning requirements for all of Chula Vista's departmental IT requirements, thereby preventing duplication of network capital and staffing resources within multiple departments. This will in turn reduce the effort required to deploy network changes and troubleshoot problems. This will allow City IT, Traffic Engineering, and the Police Department to independently manage their unique departmental applications even while they operate on a single integrated network infrastructure.

Action Item 5: Integrate Existing Traffic Control Networks into the New DNA Infrastructure

To realize the benefits of an integrated fiber infrastructure managed by Cisco DNA as described above, Traffic Engineering must work with City IT and NICP to integrate future and existing signal control networks into the new architecture. Future signal network conversions should specify appropriate DNA-compatible Cisco switch hardware for signal control cabinets with single mode fiber interfaces. Traffic staff will continue to coordinate with City IT, and other software and hardware partners to define equipment standards, deploy new network hardware, and plan/perform conversions of signal control facilities to Ethernet over fiber.

For the existing twenty-five (25) fiber-based signals, the engineering design recommended above should re-configure the 288-count fiber to terminate in one of the network aggregation points

and make appropriate fiber assignments for transport rings and laterals. Production traffic control services should then be migrated to the new configuration through coordinated planning with City IT and NIC Partners.

All new fiber-based signal networks will be constructed per the engineering design with signal control switches configured to communicate within the defined layer 2/3 architecture at implementation.

Action Item 6: Collocate in a Commercial Data Center for Direct Access to IP Service Providers

The City should explore leasing dark fiber from the San Diego fiber routes to one or more commercial data centers located in San Diego to obtain direct access to collocated internet service providers, Microsoft Azure Express Route providers, and other potential next-generation telecommunications services. Once connected at these Internet POPS, internet bandwidth can be obtained at less than $0.60 per megabit for one GB Ethernet[1] from providers such as Cogent and Hurricane Electric. Direct peer IP services are less likely to be affected by fiber cuts and equipment failures, lending to a more reliable service experience. In addition, collocation from a network services provider such as Crown Castle could provide a secure off-site location for disaster recovery. Options for commercial data center collocation and service peering are provided here for further research.

[1] Hurricane Electric, 1 gigabit ethernet, burstable to 95 percentile.

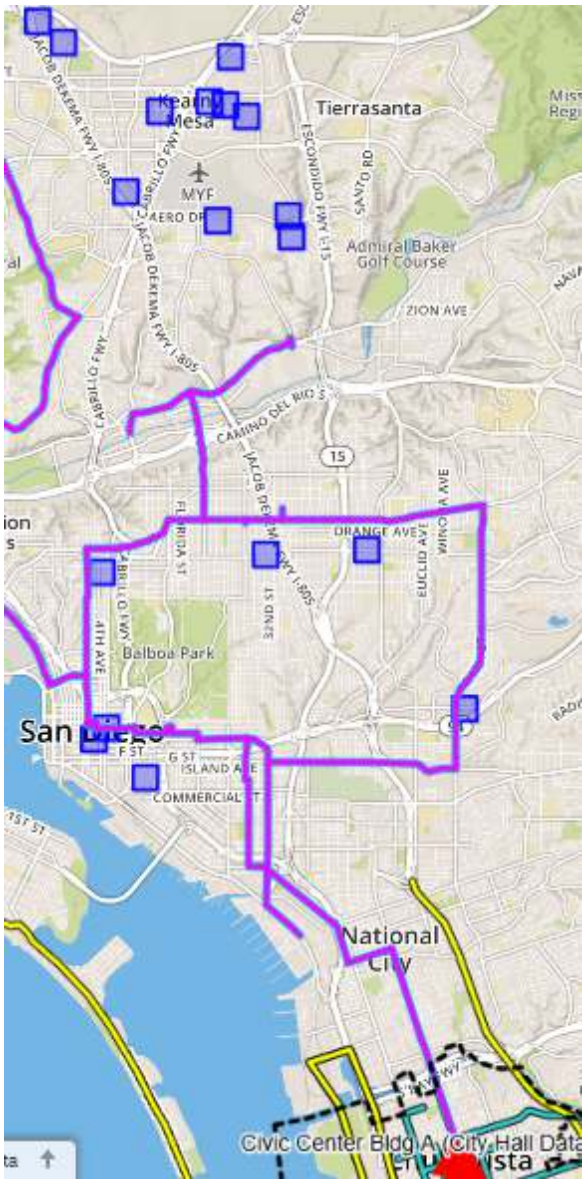


Figure 2-11 Data Centers and Fiber in San Diego

Table 2-13 Data Centers in San Diego

Provider	Address	Tenants
Crown Castle #1	3180 University Avenue, San Diego, CA	Cox, Global Crossing, Level 3, CenturyLink, Crown Castle
Crown Castle #2	8929 Aero Dr, San Diego, CA	Cox, Global Crossing, Level 3, CenturyLink, Crown Castle
Crown Castle #3	8830 Complex Dr, San Diego, CA	Crown Castle
Crown Castle #4	8971 Complex Dr, San Diego, CA	Crown Castle
Crown Castle #5	9276 Scranton Rd, San Diego, CA	Crown Castle
EdgeConneX EDCSDG01	5761 Copley Dr Suite 150, San Diego, CA	Various
Scale Matrix	5775 Kearny Villa Rd, San Diego, CA	Zayo, Cox, CenturyLink, Crown Castle
zColo Collocation	9606 Aero Dr, San Diego, CA	Zayo, Cox, RedIT, Crown Castle
SimpleNet Collocation	225 Broadway, San Diego, CA	Various
American Internet Services #1	9305 Lightwave Ave, San Diego, CA	Zayo, Cox, American IS, Zayo, Crown Castle
American Internet Services #2	9725 Scranton Rd, San Diego, CA	Cox, American IS, Crown Castle
Cogent	525 B St #1020, San Diego, CA	Cogent, various

Table 2-14 Summary of Fiber Network Metrics, by Ring, by Phase

		Core / Backbone		Laterals / Distribution		Core + Laterals	
Ring	Phase	Linear feet	Linear miles	Linear feet	Linear miles	Linear feet	Linear miles
1	1	73,371	13.90	2,539	0.48	75,910	14.38
1	2		0.00	112,855	21.37	112,855	21.37
1	3		0.00	35,953	6.81	35,953	6.81
2	4	70,343	13.32	31,332	5.93	101,675	19.26
2	5		0.00	81,280	15.39	81,280	15.39
3	6	32,953	6.24	17,971	3.40	50,924	9.64
		176,667	33.46	281,930	53.40	458,597	86.86
		38.52%		61.48%			

2.5 FINANCING OPTIONS FOR CONSTRUCTING FIBER RINGS

Alternatives for funding the development of Ring 1 (required) and Rings 2 and 3 (each required, and contingent on funding) are outlined in the Long-Term Costs section.

2.6 CONCLUSION

The recommendations for core and LAN/MAN improvements are complex and costly but are well worth the investment of capital and resources to accomplish over the long term. An integrated network infrastructure with centralized management and security allows the City's IT resources to be leveraged across all departments while minimizing duplicate effort and cost. Furthermore, the City will reap increased efficiencies through an integrated IT infrastructure that improves network scalability, performance, interoperability, usability, reliability, security, and operations in the following ways:

1. *Scalability:* The new network can easily scale by increasing optical bandwidth, network capacity, and fiber extensions through incremental capital investments and equipment reconfigurations. This will allow the City to grow the network in lockstep with the continually changing demands of IT applications and services.
2. *Performance:* End-to-end performance will improve by nature of standardized circuit types and a low latency layer 2/3 architecture operating on a 40 Gbps transport ring for access to data centers and internet services.
3. *Interoperability:* The City's standards-based integrated network will support all departmental applications and allow for centralized management and security.
4. *Multi-use:* The integrated network will leverage common assets and staffing resources to support both common use and unique departmental applications.
5. *Reliability:* The new fiber ring, MPLS transport, diverse laterals, and Cisco DNA platform will all lend to much higher reliability of the network through controlled change management, protected transport, and P1/P2 service redundancy.
6. *Security:* Security of the network will be much improved through migration to private fiber and the implementation of Cisco DNA for security policy and threat management.
7. *Operations:* Overall network operations for City IT will be simplified through Cisco DNA-controlled change management and standardized components. Operations will be simplified for Traffic Engineering by allowing their staff to focus on the traffic applications instead of the communications networks supporting them.

2.7 ALTERNATIVE SOLUTIONS FOR FIBER NETWORK

In addition, Magellan recommends that Chula Vista consider issuing an RFP for alternative fiber solutions, seeking responses from additional respondents who may wish to contribute to City's economic development and communications needs.

3. Data Center

3.1 BACKGROUND

The City of Chula Vista's current data center provides adequate protection for the City's basic services and can absorb additional capacity for growth. It is recommended that a comprehensive review of the existing controls be reviewed to ensure the physical and environmental controls are adequate while also supporting the capability for business resiliency.

3.2 DATA CENTER IMPROVEMENT PLAN

The following controls should be implemented and reviewed annually to ensure adequate protection:

City of Chula Vista should take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage to the City's physical premises, systems, and information. City of Chula Vista should also take appropriate steps to protect against environmental and systems malfunctions or failures.

The following table summarizes the several additional policies and procedures that should be implemented to create a world-class data center operation supporting today's needs and tomorrow's fiber and Smart City initiatives.

Detailed checklists of information to be created for each policy and procedure may be found in Appendix B – Data Center Support.

See Table 3-1 beginning on the following page for the datacenter control matrix.

Table 3-1 Datacenter Control Matrix

	Data Center	Objective	Risk Statement	Control
3.1	Environmental Controls	Implement critical supporting utilities, such as climate control, fire suppressants and backup power supplies needed to support the business operations.	Absence of environmental controls may result in the organization being more susceptible to business interruptions.	Facilities housing mission data, scoped systems and or physical media are protected with environmental controls.
3.2	Physical Security Controls	Ensure that physical access to data or systems is restricted by layered security controls and that only authorized personnel are allowed access to restricted areas.	Absence of physical security controls may result in impairment, damage or destruction of physical plant and human resources. Likely impacts to business operations may result.	Facilities housing scoped data, scoped systems and physical media are protected with physical security controls.
3.3	Secure Workspace Program	Ensure that protecting the secure workspace environment is part of the physical security and risk management programs.	Absence of a secure workspace program may result in the organization's inability to identify appropriate procedures to secure the workspace environment.	Formal enterprise risk governance program is aligned with the business environment and organizational strategic objectives.
3.4	Secure Workspace Perimeter	Control ingress to and egress from the secure workspace. The level of controls should be commensurate with the level of risk.	Absence of a secure workspace perimeter may result in the organization being more susceptible to unauthorized access to facilities housing scoped data, systems or media.	Implement physical security control features to control ingress to and egress from the secure workspace.

	Data Center	Objective	Risk Statement	Control
3.5	Secure Workspace Access Reporting	Maintain access reports.	Absence of access logging management may result in the organization's inability to identify or report unauthorized access to secure workspaces.	Access to secure workspace is logged and reports are maintained.
3.6	Secure Workspace Compliance Inspections	Complete periodic compliance inspections of the secure workspace desktop environment.	Absence of compliance inspection for the secure workspace desktop environment may result in the organization's inability to identify ineffective practices, and loss or compromise of information or assets.	Conduct periodic compliance inspections of the secure workspace environment.
3.7	Visitor Management	Establish a visitor management program.	Absence of adequate visitor management procedures may result in unauthorized or unsupervised visitor access.	Establish process and policy for visitors to the facility, including requiring visitors to present valid government-issued ID and display a visitor's badge at all times.

	Data Center	Objective	Risk Statement	Control
3.8	Business Resiliency	Create and maintain in-depth business resiliency governance policy, function and processes that documents overall expectations for the program, how the program is to be executed and defines responsibility for each element of the program.	Absence of a business resiliency governance policy to guide the risk management program may result in a lack of clear direction and senior management involvement to assure readiness to handle service disruptions and impact to the products and services provided by the organization.	Create formal policy that establishes program objectives, responsibilities and processes.
3.9	Business Impact Analysis (BIA)	Conduct an assessment to prioritize all business assets and activities, including their interdependencies, as part of a workflow analysis. This assessment should evaluate the potential impact of business disruptions resulting from uncontrolled, non-specific events on the organization's business functions and activities.	Absence of a business impact analysis may result in lack of prioritization of business assets and activities, which could in turn prevent the necessary assets and activities from being prepared to respond to a business disruption that impacts the continued availability of critical products and services.	Perform, maintain and periodically exercise (minimum annually) business impact analyses (BIA), and upon material changes to critical business functions and their required assets and dependencies. Senior management review of results.

	Data Center	Objective	Risk Statement	Control
3.10	Risk Assessment	Create and maintain an in-depth business risk assessment that identifies and analyses the likelihood and impact of disruptive incidents to the organization and its clients/customers.	Absence of a risk assessment program may lead to unidentified threats and treatments that result in business disruption.	Catalog and maintain the critical resource dependencies identified by the business impact analysis. Senior management review of results.
3.11	Business Activity Level Recovery Planning	Create business recovery plans that will effectively guide the recovery of the critical business activities identified from the Business Impact Analysis.	Absence of formal business recovery plans may result in critical business activities not being recoverable within needed timeframes.	Business recovery plans are developed, maintained and reviewed periodically (minimum annually). Senior management review of plans.
3.12	Backup Media Creation and Restoration	Systems, applications and data must be available in event of an incident that compromises or impairs production information technology operations. Backups or replications of scoped data should be available to meet required Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).	Absence of processes and capabilities for the restoration of scoped data and software may lead to a loss of ability to resume operations and the provisioning of services in the event of corruption or loss of the primary data source.	Implement backup or replication process for systems, applications and data to ensure successful restoration. Periodically test. IT management review of test results.

	Data Center	Objective	Risk Statement	Control
3.13	Disaster Recovery, Business Continuity Testing	Conduct thorough exercises that validate the effectiveness of business continuity and disaster recovery procedures and capabilities, the readiness of its personnel to perform required actions and the viability of related communication mechanisms and procedures.	Absence of exercising and testing may lead to unprepared individuals, unanticipated delays in meeting recovery objectives, and/or unidentified gaps in the program.	Business resiliency and disaster recovery exercises are defined, scheduled, planned, conducted and evaluated according to a consistent process. The problems identified are made visible and documented with an associated remediation action plan.
3.14	Infectious Disease Planning	Create and maintain infectious disease outbreak plans which consider outbreaks impacting internal parties, third parties and customers.	Absence of formalized process to respond to infectious outbreaks could result in the inability of the organization to continue to provide its products, services and related support or to adapt to changes in demand by users impacted by an outbreak.	Establish infectious disease plan to define how the organization will prepare for and respond to the pandemic and epidemic outbreaks that may or do impact the organization, its personnel and ongoing operations.
3.15	Business Insurance	Ensure all applicable insurance coverage(s) is defined and outlined within the business resiliency plan.	Absence of insurance could result in a financial loss to the City, putting at risk its ability to resume services to their users in a timely manner.	Insurance coverages held by the organization are defined and outlined within the business resiliency plan.

4. Telephony

4.1 BACKGROUND

The term *telephony* connotates traditional phone calls using a fixed or mobile device to talk with another party. However, telephony in the modern sense is much more than voice conversations. It refers to a "Unified Communications" paradigm that includes not only an ecosystem to support voice communications, but systems to support all kinds of communications, of which voice is just one aspect. Unified Communications ("UC") allows users to communicate in many forms, including via a landline phone, mobile smart phone, email, text messaging, tablet or other device. The freedom to use many communications modes allows users increased efficiency and improved service delivery.

Unified Communications is made possible by having a common platform that all devices use, which is known as internet protocol ("IP"). UC allows for new efficiencies in the way we communicate and work. Voice over internet protocol ("VoIP") is only one component in the ecosystem that is Unified Communications. Subscribing to, managing and implementing one data network that supports all an organization's communications needs has provided the ability to cut costs and improve services.

Using UC, a variety of enterprise communication services including instant messaging, VoIP, mobility features, audio, web and video conferencing, data sharing, and unified messaging are integrated across many media types and devices. Some of the features it enables includes mobile uses such as extension mobility and single number reach. It allows users dynamic messaging options such as sending messages from one medium to another, or routing calls and voicemail communications based on the user's presence information. UC contains a set of evolving technologies designed to automate and unify communications across media and devices, allowing for reduced latency and dependence on individual devices, and enhanced mobility and business processes.

4.2 GENERAL REQUIREMENTS

Telephony has come full circle in the evolution of Hosted vs On Premise support for communications. With much better internet connections and increased migration to the "cloud," VoIP hosted solutions are becoming more cost competitive while maintaining the calling features end users desire. Many organizations are moving towards VoIP solutions hosted by a VoIP provider. Some of the pros and cons are highlighted below.

IP-based models incorporate not only hosted versus on-premises solutions, but a variety of options for implementing solutions at various stages. For instance, many organizations elect to keep their existing phones instead of going through the expense of buying all new IP-based phones by using a less expensive on-premises "box" (called an Integrated Access Device – "IAD") to convert voice calls into data packets. This can be used in a phased implementation of VoIP.

Other companies are only using VoIP for connections between their offices and the phone company's central office.

Hosted private branch exchanges ("PBX's") or hosted VoIP is a model in which the phone equipment is housed and managed by a carrier at their location. These providers then handle all the software and feature upgrades, redundancy, backup and connectivity to the internet. All the local office IP phones are then connected to a router and aggregated before being sent to the provider using a common protocol. These providers usually charge a monthly fee, per phone, for their services. It can be as little as $15 per phone to over $50 per phone per month, depending on agreements, number of phones and features required. They may also charge a fee for the number of minutes used.

On-premises solutions, on the other hand, require the equipment to be located onsite and managed by the City. The City will have gateway equipment onsite that connects to either a traditional provider to route the calls, or to an IP-based provider using SIP trunks (more on SIP later) to facilitate call completion.

Purchasing an on-premise IP-PBX phone system involves buying hardware, which includes a server with the proper number of interface cards (if needed) to be able to connect the telephone company with the IP phones. Hosted IP-PBX only involves purchasing IP phones, though a router and network switch may be needed to ensure there is one specifically dedicated to VoIP.

Below are some important considerations in deciding between hosted IP and on-premise IP options.

4.3 HOSTED VS ON-PREMISE TELEPHONY – COMPARATIVE COSTS

Table 4-1 Hosted vs On-Premise Telephony – Comparative Costs

	Hosted Private Branch Exchange (PBX)	On-Premise PBX
Costs	• Lower initial equipment cost and set-up cost. • Network qualification is performed by the customer; any upgrades are at the customers expense. • All IP-PBX feature programming is done by the customer. • No maintenance costs of the IP-PBX, but support of all on-premise and remote phones and network devices are the responsibility of customer. • Staff training is the responsibility of the customer. (Many providers offer train-the-trainer services, allowing CV staff to provide local training. • Low monthly service cost. • Easy to add extra lines. • Upgrades and new features are included. • Extended features, like conferencing, may come with additional costs.	• Higher initial cost and set-up cost. • Potentially higher maintenance costs. • Lower monthly cost after expenses are covered. • Ability to SIP trunk to get lower cost calls. • On-premise IP-PBX provider will qualify network. • On-premise IP-PBX provider will install and program IP-PBX. • On-premise IP-PBX will train staff on feature use and "best practices".

IP phones can be identical regardless of layout. For example, the 12 Polycom 550 SoundPoint IP phones can be used for on-premise IP-PBX phone systems as well as hosted IP-PBX systems. The other equipment, such as server, software, routers, switches and battery backup can be very specific for the individual system. $3,000 to $5,000 is typical for purchasing a server with the necessary software and cards. Ongoing server maintenance with hosted PBX will be the responsibility of the provider. If purchasing an on-premise PBX, the cost becomes the burden of the owner, if not included in the IP_PBX package.

4.4 HOSTED VS ON-PREMISE TELEPHONY – PROS AND CONS

Table 4-2 Hosted vs On-Premise Telephony – Pros and Cons

	Hosted Private Branch Exchange (PBX)	On-Premise PBX
Positives	• Providers have more resources than users, so new feature sets are possible. • New feature installation is handled by provider to avoid confusion. • Picking and canceling virtual numbers is easy and fast. • Moving a phone system is easy; IP phone is plugged into a broadband connection. • Hosted provides edge border controllers or various other kinds of NAT software to help navigate routers. • Patches and upgrades of the IP-PBX are handled by the provider. • Loss of Internet or catastrophic event has no effect on operations because calls can be sent to voice mail or a mobile phone (due to an off-site facility that has safeguards including back up power sources).	• Having on premise PBX gives user control to create, adjust and delete users as desired. • New open source feature sets can be added without any license fees. • Current carrier does not have to be changed. • VoIP trunks can be added to save on calling costs. • Server ownership reduces expenses over time. • No do-it-yourself time on the part of the customer. • Professional training of staff on new IP-PBX system is handled by the provider. • With SIP trunking, loss of Internet or catastrophic event has reduced effect on operations because calls can be sent to another number or a mobile phone (due to failover capability at an off-site facility that has safeguards including back up power sources)
Negatives	• Connections and voice quality are a result of internet connection. • Loss of Internet results in loss of phone service (settings can be adjusted so that it goes to voice mail or routed to a cellphone). • Flexibility of system is limited. • Customization of features may be slow or unavailable depending on provider. • Fees can be increased, and cancellation fees can be charged. • Stability of provider may vary within operations and finance.	• On-premise IP-PBX needs a provider who can manage it properly. • Expansions may result in complicated projects depending upon the provider. • On premise IP-PBX manufacturer could go out of business, leaving problems with managing root problems. • Technician may need to be called for upgrades and patches on software (and costs can be incurred). • Loss of power or PBX failure will result in callers not being able to get through, which stops business operations unless you have a SIP provider. • Additional ITS staffing, expense required.

All of the feature sets and reports are managed the same way in either a hosted or premise-based solution by using a GUI software interface. This interface allows network managers and even the end user to select which features to implement including the setup and facilitation of conference calls and/or video chats, call routing rules, security (encryption types, users access, HIPPA compliance), VM access, call attendant and many others. Usability is quite simple.

VOIP Features

Most VoIP providers, whether hosted or on premises, offer a set of features and benefits with their product offerings. Some of the most common features are:

a. Caller ID
b. Call forwarding - ability to forward all calls to an end users' choice of device
c. Call waiting
d. Call blocking
e. One-click dialing via integrated software app
f. Three-way calling
g. Conference call set-up and facilitation
h. Video chat and conference video chat
i. Collaborative presentations
j. Long distance. Sometime free, sometimes for a fee after a certain number of minutes
k. Music on hold with scheduled end user selectable music or advertisements
l. Instant messaging
m. Contact Center
n. Call Logging/Recording
o. Voicemail to text and text to voicemail
p. Call attendant capabilities
q. Automated call distribution – for service center groups.

Given that most VoIP solutions offer nearly identical features, much of the decision about one solution vs the next revolves around cost, customer support and supported devices and whether they use proprietary solutions.

4.5 CURRENT ENVIRONMENT

The City of Chula Vista has an aging (15-20-year-old) NEC based voice solution today. This system is becoming increasingly difficult to support in terms of staff expertise, parts replacement, and modern functionality. The system has limited support for Unified Communications and limited support for IP based solutions, although some City rec centers and one fire station have IP services, with limited support.

This current system has an annual contract of roughly $30,000 for support, but that does not include onsite setup, moves, changes, adds or deletes. Because the system is predominantly an older PBX solution, any changes or moves will require a physical modification to the twisted pair

wire and phone jack the phone is connected to. This creates additional time and cost (labor) for each needed change in phone support.

The City has the equivalent of one-half Full Time Employee (FTE) to support but acknowledges it could use some additional staff to meet service level agreements. Staffing/expertise is getting more difficult to find given the age of the current system.

Moving to a UC solution will help the City improve services to the community and provide the City employees with additional tools to enhance productivity for the benefit of the City as a whole. Money and time can be saved by simplification of moves/adds/changes, through access to video chats, conferencing tools and the ability for workers to select the device/method of their choosing for communicating with others including phones, cell phones, laptops, tablets or other devices. Additional productivity will be gained with an expanded feature set available to the City including voice-to-text, text-to-voice, call attendant features, call recording and one-click dialing to name a few.

4.6 CLOUD-HOSTED VS ON-PREMISE COST ESTIMATES

Rough cost estimates for a cloud-hosted solution include:

- $10 per month per user or $15,000 per month for 1,500 phones ($180,000 annually)
- Limited staffing
- Monthly SIP trunk costs
- All costs are operating expenses

Cost estimates for an on-Premise solution include:

- $300,000 for new phones
- $55,000 new server, gateways, firewalls and software
- 2 FTE staff ($250,000 annually)
- Ongoing upgrades maintenance agreements - $5,000- $7,000 annually
- Training
- Monthly SIP trunk costs
- All costs are likely operating expenses, including phones (due to low unit costs)

The City already has power over Ethernet (POE) switches at each location, so installing and using new IP based phones should be straightforward.

4.7 NEXT STEP TACTICS AND TASKS

4.7.1 Issue RFP to Identify VOIP Solution

Chula Vista should develop and issue an RFP to identify possible solution providers for a City-wide VoIP. The selected respondent would provide all installation, deployment, configuration, and support services. Solutions could be provided on an in-house or cloud basis.

The City should use a cloud-based hosted solution paid via a monthly Op-Ex expense. Many vendors provide both a hosted and on-prem solution, so selecting a vendor should include looking at all available options including price, support, ease-of-use, feature set, security and monthly recurring costs (MRC). The City should develop an RFP to determine the solution to be used.

As demonstrated above, the labor costs for supporting an on-prem solution can be quite large relative to the hosted solution. However, hosted solutions do come with a smaller up-front fee for hardware and software but typically have higher per user MRC. Staffing issues are a concern for nearly every municipal entity, so we strongly recommend a hosted IP solution paradigm.

Finding the Right Solution

There are many VoIP and Unified Communications providers to choose from. Below is a list of some of these providers and are listed in no particular order of preference or recommendation. Vendor selection should be done through an RFI process. Magellan recommends using one of the larger more established companies.

- Ring Central
- Cisco
- Mitel
- Vonage
- Nextiva
- Jive
- 8X8
- Digacom
- Ooma Office
- Others

There are also providers of IP based phones and handsets including:

- Polycom
- Avaya
- Yealink
- Panasonic
- Mitel (ShoreTel)
- Jabra
- Sennheiser
- Grandstream
- Others

Most of these vendors make a broad range of phones and features as mentioned above. There is no shortage of vendors supporting IP phones and UC solutions.

5. Video

5.1 BACKGROUND

Video is essentially human-viewable light sensor data. The charged coupling device at the heart of digital video cameras is simply an array of capacitors that translates photons into electrons—"sensing" light—which are digitized by the camera's electronics to create pixels. A series of images composed of these pixels creates a video stream. Artificial intelligence and basic pattern recognition technologies can be applied to resulting data to analyze images. Data about the video (metadata), including date/time, location, source, etc., can be embedded in the video stream for additional forms of analysis. Video analysis possibilities depend on the camera's field of view, optical quality, resolution, and characteristics of the CCD (type of light sensed, for example, infrared or ultraviolet). While video is amenable to extreme data compression, video streams constitute relatively large data loads for processing, transmission, and storage.

Magellan Advisors interviewed key department representatives on their current use and future video requirements for internal and external operations purposes. We evaluated the City of Chula Vista's camera system components, including the video management system (VMS), reviewed proposed camera locations, and considered the impact of expanded video use on the City's website and network. Site-specific information necessary for basic camera installation at surveyed sites is attached in Appendix C.

5.2 GENERAL REQUIREMENTS

There should be surveillance cameras at all City facilities covering access/entry points, major corridors, elevators, critical areas within the buildings, parking areas, and public areas on City property outside the buildings. There may be cameras in public spaces adjacent to key commercial and institutional sites, areas with high incidents of criminal activity, or in other locations where deemed appropriate. The City should form federation agreements for sharing video feeds with key stakeholders, including places of worship, recreation, schools, and transportation. These agreements should include terms regarding appropriate usage; for example, ensuring that facial recognition techniques should not be used to identify individuals unless appropriate, controlled steps are taken. All surveillance activities should be fully vetted with stakeholders unless conducted covertly with warrant by sworn law enforcement officers.

Police and other sworn officers are required to wear body-mounted cameras, and vehicles—at least those used for public safety—may have front-facing cameras. Various public meetings may be video streamed for live broadcast/streaming and/or recorded for future reference. Closed meetings may also be videoed with proper authorization but should be securely stored and reviewed for public disclosure.

Video feeds should be aggregated to at least two locations, including central dispatch, for monitoring. Some feeds may be aggregated for special purposes, such as monitoring facilities for

maintenance needs. The City should have well-defined procedures in place for monitoring or reviewing video feeds.

Selected feeds should be stored for at least 24 hours, and some feeds—particularly any with evidentiary value—should be archived. The City should develop video archival and retrieval rules to ensure evidentiary value and privacy of persons captured in videos are preserved.

5.3 CURRENT SITUATION

The Police Department was installing cameras at the time of this analysis. The department's headquarters at 315 Fourth Avenue has 140 cameras inside; four are being installed outside the building, and the police have cameras at three other locations: the animal shelter, Fire Station 7, and the Otay Ranch Shopping Mall. All officers have body cameras that off-load their video when returned to dock. They do not have vehicle mounted cameras. One mobile command center has a camera. Police drones generate video, which must be downloaded and stored (to the Genetech system) at the end of a mission. All regional public safety agencies have shared access to video camera streams.

The Chula Vista Police Department recently deployed four pole-mounted cameras that connect via Verizon and were federating traffic cameras. The Police federate cameras at the Port of San Diego and have means to do so with other entities (MTS? Others?). With the exception of Police Axon body worn cameras, video of which is stored off-site at Taser's Evidence.Com secure off-site repository, and is managed by the Police Department, the rest of City of Chula Vista video is managed and stored via Genetech (https://www.genetec.com/) and via Livestream (https://livestream.com/). Video is archived for evidentiary purposes based on the City's standard document retention policies. The City's Real-Time Crime Center has video analytics capabilities (also ability to analyze other sensor data).

Most other City departments do not have or operate cameras. The Fire Department should have cameras at its nine stations, warehouse, training division, prevention office (610 Bay Blvd.). It also needs remote mobile video from drones, vehicles, or other apparatuses for scene assessment. The City Library's two branches and one satellite location should have video for surveillance per the general requirements discussed above. These departments, as well as others, could benefit from use of video for communications and training purposes. These video feeds will generally not need to be archived but could be monitored only for performance or other review purposes (e.g., remote arraignments, real-time telehealth assessment).

The Traffic Department has 273 signals and 9,000 streetlights. Most traffic signals are connected via telephone line. Twenty-eight have been converted to adaptive signals with the addition of cameras and other sensors and are connected via fiber. High-definition pan-tilt-zoom (HD PTZ) cameras will be incorporated into every signal as it is added or modified, connected by fiber and/or wireless communications. The video is fed to the Traffic Management Center and should eventually be available via mobile. The Traffic Department does not use any facial, license plate,

or other recognitions technology, although their cameras are capable. This would be a Police Department function, if it were deployed.

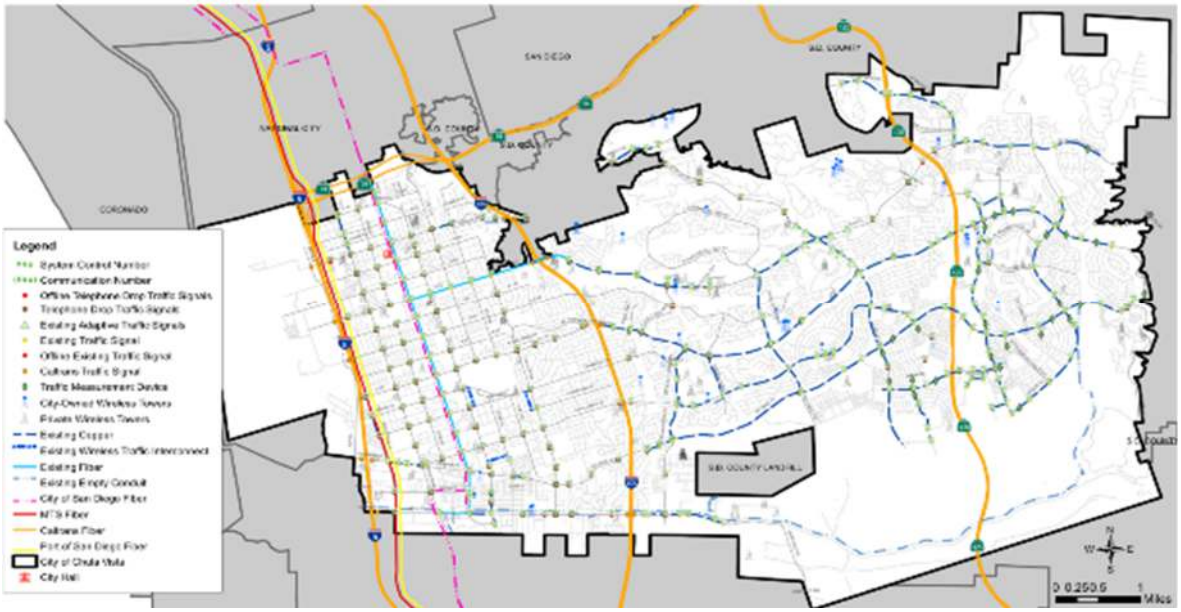


Figure 5-1 Existing Traffic Systems Communications Network (Source: City of Chula Vista)

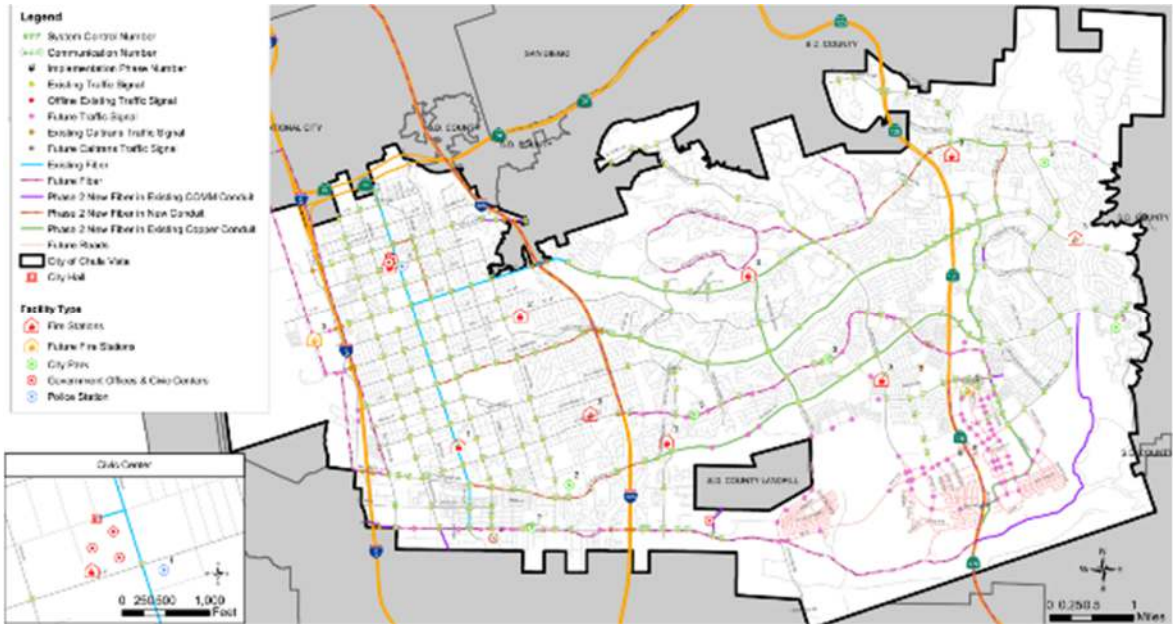


Figure 5-2 Traffic Signals – Planned

5.4 NEXT STEP TACTICS AND TASKS

To maximize the efficient, effective use of cameras, the City of Chula Vista should:

- *Develop phased implementation plan for new, upgraded cameras – ITS-led.*
- *Coordinate camera deployment with other technology upgrades*, particularly to access control systems and network infrastructure (especially Wi-Fi).
- *Identify network requirements for camera backhaul and signal aggregation points* for prospective camera systems/technologies, consistent with implementation of proposed fiber networks.
- *Establish policies for aggregating, monitoring, retrieving, storing and sharing video content* consistently across all departments, for all purposes, based on current best practices.
    - Policies should distinguish between video for communication and video for surveillance, between surveillance for resource/traffic management and crime suppression/security, and for levels of sensitivity and privacy requirements.
    - Use a single standard system for these purposes. Ensure that system is flexible, open, and portable to avoid excess costs and technological lock-in.
    - Ensure audit trails are maintained for all video segments viewed, shared, archived, or extracted.
- *Ensure network infrastructure provides direct, wired access to cameras* or video aggregation points. Refer to the list of sites in appendix C.
    - Prioritize camera deployment based on available funding and strategic goals.
- *Reach out to additional stakeholders to establish federated video sharing agreements*; consider establishing a formal program whereby private citizens and corporate entities can federate their video.
    - Establish requirements and specification for City video systems to take in federated video streams from private or other entities
    - Develop policy for sharing video streams, on request or as standard operating procedure.
- *Develop systems for securely accessing video feeds and delivering video to remote users* in alignment with goals and priorities (i.e., customer service, emergency response, performance reviews). Include chain of custody considerations.
- *Develop storage, retention, and archiving strategy and policy for all video –* consistent with data policies, access policies.

6. Signage & Kiosks

6.1 BACKGROUND

Digital signs are simply computer display. Kiosks have basic input mechanisms—a touch screen, for example—to create an interactive display. The key to both is content that is structured for interactivity. A basic display might have different messages at different times, which means the messages must be programmed with a means to change them. The simplest sign example might be an "open" / "close" sign: turn it on during business hours; turn it off outside of business hours. A parking pay station is a prime example of a kiosk, although the most effective and economical kiosks may support multiple functions (for example, pay for parking, report a public works issue, or summon emergency assistance from a single kiosk).

The more complex the purpose of a display is, the more complex its content and functionality must be. A traffic display might have automatic messages for traffic or weather conditions, calling for the need to distinguish between types of precipitation, wind speed, or temperature. The display must have the relevant messages and means (i.e., sensors) to trigger changes. Complex content typically requires human interaction or intervention. A directional display, for example, might have means for a visitor to converse, or otherwise communicate, with a customer service representative or other guide. This functionality must be programmed into the system, and there must be a person with whom the user can interact. It is important to understand that displays and kiosks must be highly focused and task oriented. People refer to or use them for very specific purposes. Systems that are clearly focused on user's purpose can cause confusion, frustration, or worse.

6.2 GENERAL REQUIREMENTS

The City of Chula Vista's requirements for displays and kiosks depends on how and where the City needs to inform citizens and visitors about activities, the status of assets, and other issues. Information for motorists must be clear, simple, and visible. Information for pedestrians must also be clear but allow for great depth via interaction. Task- or transaction-oriented kiosks are required for public venues and citizen-facing departments.

Most any mobile app (i.e., municipal software for smartphones) may benefit from a kiosk-based version to ensure equitable access, and just for public convenience. The functions of ACT Chula Vista and the SDMTA website, for example, may be deployed to kiosks. By the same token, kiosks must be accessible for persons with cognitive and physical handicaps and should be accessible to persons who do not speak English or who are unfamiliar with local culture. The kiosks may function as network infrastructure for public Wi-Fi hotspots, and may generate advertising and convenience fee revenues for the City.

The network requirements of displays and kiosks depends on (a) the criticality of (b) the content, information, or messages, and (c) how much it changes, particularly in response to (d) people

interacting with it or (e) other external stimuli. Most displays have relatively low content requirements, such as traffic information displays. Such displays change with moderate frequency in response to centralized control, and are essential to safe, unimpeded traffic flow. Kiosks for tasks such as paying fees and fines, reserving facilities, or setting appointments are less critical and can involve highly variable and rich information. Some functions—summoning emergency assistance, for example—can be critical but most are for convenience and efficiency.

It may be best to connect traffic information signs to fiber for high reliability, while connecting kiosks to wireless for flexibility. Generally, the network connections for displays/kiosks may be via reasonably high-speed wireless, although some pre-programmed signs may only need very low-bandwidth connectivity to change the messages or their timing. Kiosks can provide enhanced internet access, particularly in lower-income neighborhoods, if used as Wi-Fi access points, which would require reasonably fast backhaul as well as means to authenticate users and push custom content to them.

6.3 NEXT STEP TACTICS AND TASKS

To maximize the efficient, effective use of signage and kiosks, the City of Chula Vista should:

- *Plan for motorist-targeted displays* for parking on every block in commercial districts and densely populated areas, and for travel information approximately every half-mile along major thoroughfare.
    - Design travel-related displays for high-reliability, including for man-made or natural disasters.
    - Combine and/or align parking and travel displays where appropriate, i.e., major thoroughfares through commercial districts.
- *Plan for at least one kiosk at all public buildings and every major park*.
    - Incorporate the full range of appropriate functions, across local and regional agencies. For example, a kiosk at the courthouse should give users access to building security, court dockets, mass transit, and parking.
    - Consider simplified kiosks (for emergency calls, parking, and other basic information) for all parks, along pedestrian paths/routes, and in commercial districts and densely populated areas.
    - Design kiosks around specific activities or tasks, incorporating as many into the system as practical without reducing usability or usefulness.
- *Decide whether kiosks are to be used to for public Wi-Fi*, and whether there is a digital equity goal for this purpose. If so, identify locations where additional access is required such as near community anchor institutions and in public gathering places.
    - Develop a public Wi-Fi business model and program, including funding via advertising and sponsorships.
- *Review funding for infrastructure that may be used to connect displays and kiosks* for various purposes to ensure they are not disallowed by funders.
- *Determine the variability, criticality, and level of control required* for each class of display or kiosk, and design or select hardware and software accordingly.

- *Establish a comprehensive but limited set of standards* for all displays and kiosks, allowing for secure data flows into each from sensors, other systems, and people, and update automatically.
    - If there is a vehicle wreck, for example, traffic displays may need to automatically inform motorists, allow police to send detour information, and update relevant bus schedules.
    - All displays and kiosks should be minimally integrated and centrally controllable for emergency response and similar contingencies.
    - Ensure standards and underlying technologies are flexible and open to avoid incompatibility and lock-in with a particular vendor.
    - Display must conform to Manual on Uniform Traffic Control Devices (MUTCD) guidelines (https://mutcd.fhwa.dot.gov/).
    - Displays may utilize International Standards Organization (ISO) standards for intelligent transport systems (https://www.iso.org/committee/54706.html).

7. Sensor Networks

7.1 BACKGROUND

A sensor is a device that converts energy—from chemicals, light, movement, pressure, temperature, etc.—into digital data or signals, basically measuring some form of energy. Sensors are often combined with servomechanisms (or just "servos"), which translate signals into physical action. Sensors make it possible to automate activities or events, do them on-demand without human intervention, and greatly reduce labor requirements. For example, a door-opening servo be combined with a pressure sensor or a retinal scanner, depending on access requirements. When the sensor generates a particular signal, the servo opens the door. Alternately, the signal might result in a security alert, a "this area closed" message, most any other output required to achieve a result. Sensors are often deployed in arrays and networks. Multiple sensors in an array can measure a particular form of energy over an area or capture various forms of energy (light, movement, and temperature, for example). Devices, including cars and smartphones, have sensors built into them and can act as sensor as they send data to a network. A sensor network interconnects multiple sensors throughout an area.

7.2 GENERAL REQUIREMENTS

The City of Chula Vista does not have well-defined requirements for sensors because the technology is reasonably new. Recent planning documents identify applications and requirements for sensors, and that sensors and machine-to-machine communications represent a fundamental difference between Smart City infrastructure and traditional municipal IT. The "Smart Bayfront" is envisioned as a particular sensor-rich environment, according to these documents, in which "[t]he current network does not have the scalability to meet the connectivity needs of these new services."[2]

Generally, sensors require means to acquire and aggregate the data they generate. Due to the distributed, small-scale nature of sensors, these means are essentially wireless, though they can be fiber-based. There are numerous protocols for wirelessly connecting sensors via what is generally referred to as a low-power wide-area network (LPWAN). Some, like cellular data services are both proprietary and available only as a fee-based service with monthly recurring costs for each connection. Two such protocols are LTE-M[3], which has relatively high data rates and can be used for roaming applications, and narrowband-IoT[4] ("NB-IoT") for fixed devices that generate

[2] SBC 2-12

[3] LTE-M refers to "Long-Term Evolution for Machines" cellular wireless. For more information see https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/.

[4] IoT stands for "Internet of Things," which is a general approach to technology deployment in which practically everything is connected to the internet—via the Internet Protocol—and can send data and receive commands.

small data flows. Other technologies are proprietary but do not require a service provider. SigFox uses proprietary hardware and software. LoRaWAN is an open standard for any software but is based on proprietary LoRa chips. Weightless is an open source standard for software and hardware, much like Wi-Fi. Wi-Fi can be used for LPWAN, especially with the new low-power 802.11ax (also known as Wi-Fi 6) version of the standard.

All of these technologies require an access point or gateway to receive data from the sensors, which must have a backhaul connection, typically via cellular, fiber, or Wi-Fi. All of these standards have a range of up to 10 kilometers, with the exception of Wi-Fi 6, which is expected to have a range of about 250 meters. Bluetooth and Zigbee can also be used for sensors but have very limited range. The sensor network is expected to require security infrastructure, specifically authentication and digital certificates. This means the network to which sensors connect must have authentication services available to identify sensors and keep rogue devices off the network.

The general requirements for sensors, according to Chula Vista's prior plans and studies, relate to asset tracking, energy management, environmental sensing, solid collection. Remote management of building and utility systems seems to be the largest application area, including air pollution monitoring, energy management, leak detection, and irrigation controllers. These applications require a wide range of sensor types. Sensors will be needed in any location or on any asset that is to be monitored or tracked, including building entrances, lights, manholes, parking spaces, utility meters, vehicles, water tanks, etc., and for particular data such as motion or water quality. Available information, plans, and studies do not further define requirements simply because the City of Chula Vista, like most other cities, has not previously used or systematically reviewed uses for sensors.

7.3 CURRENT SITUATION

The City of Chula Vista has practically no current sensor technology. Therefore, and in accordance with the scope of this Plan, this section analyzes the range of Smart City Sensor Technologies that are being deployed by leading cities around the world. Amsterdam, Barcelona, London, New York, and Singapore are paving the way for other Smart Cities, and sensors are integral to their efforts. These cities use sensors to manage and regulate activities and assets, generally to protect the environment, improve mobility, safety, and transportation, and deliver utilities.

Transportation is possibly the most common application for sensors. In Barcelona, pressure sensors embedded in parking spaces track which spaces are open.[5] The data feeds digital displays and smart phone apps for drivers to find and pay for parking. Within a year of implementation, Barcelona was issuing over 4,000 parking permits per day, reducing congestion and pollution, and

[5] http://www.barcinno.com/barcelona-smart-city-technologies/

saving drivers a lot of time and frustration. The Port of Amsterdam uses sensors on mooring dolphins to identify possible damage or maintenance issues, as well as track utilization.[6] Transport for London uses sensors for humidity, temperature, vibration, and other environment and mechanical factors to proactively address issues in the Underground, the city's extensive subway system.[7] They are planning to track movement of people by capturing information broadcast by smartphones. London also uses environmental sensor in various locations—including school kids' backpacks—to target investments in mobility for maximum impact. New York has multiple mobility and transportation applications using sensors. Data from movement-sensing microwave sensors and traffic video cameras, along with EZPass readers for toll and mass transit is used to expedite buses and manage congestion.[8]

Quality of life and public safety applications go hand-in-hand. Barcelona was an early adopter of smart street lighting, using a combination of LED lights and sensors to reduce costs, environmental impacts, and public safety issues. They used sound sensors to reduce noise pollution in areas with a robust nightlife. The Sounds of New York "crowdsources" this application by making sensors available to any residents who feel they have noise problems.[9] Amsterdam has taken this one step further by using sound sensors and advanced analytics to identify altercations and underground activities before they start.[10] Gunshot detection, which also uses sound sensors, has become a popular applications in some areas. The New York Police Department deployed chemical and radiation sensors along with video and advanced analytics to reduce response times.[11]

Utilities are also a common application. "Smart Grid" electrical (now being extended to other utilities) runs on power sensors distributed throughout a power distributor's infrastructure. New York City's Department of Environmental Protection uses chemical and sound sensors for continual real-time monitoring of its water system. New York also uses sensor technology for consumer protection. The Heat Seek application uses data from temperature sensors in private residences to make sure landlords are providing heating, as required by city regulations.[12]

---

6 https://www.portofamsterdam.com/en/news-item/port-amsterdam-and-30mhz-collaborate-use-sensors-port-area

7 https://www.forbes.com/sites/federicoguerrini/2014/06/08/how-london-is-quietly-becoming-a-city-of-sensors/

8 https://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf, pages 9-10

9 https://wp.nyu.edu/sonyc/

10 https://thenextweb.com/the-next-police/2018/06/08/1128392/

11 https://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf, page 18

12 https://heatseek.org/

Singapore is using pervasive sensors to collect data about all aspect of life in the city— "Everyone, Everything, Everywhere, All the Time"—even into private residences.[13] The technology can monitor activities of older persons so they can safely remain in their homes as they age. Of course, such ubiquitous monitoring by government can be problematic, especially in societies with greater concern for privacy than in Singapore. As noted above, cities are addressing this by actively involving citizens to deploy sensors and making the data publicly available. For example, New York enables community members themselves to act as real-time sensors using their smart phones and social media, as well as specialized sensors and city infrastructure to aggregate and distribute data.[14] The Things Network, which started in Amsterdam and is now global, aggregates data from a wide range of sensors that people can place on most anything.

There are three critical considerations apparent in each of these applications. The first is the sensors themselves, including the standards they use to connect to a network and send data. The second is the network architecture: where do the sensors connect and what services they use in the process. Authentication is particularly important for data quality and security. Possibly the most critical consideration is the role of citizens. Are they data consumers or producers? If they are producers, how do they opt in and out of the network? Most people object to being surreptitiously monitored, especially if they have no access to the resulting data. Thus, it is advisable to actively involve citizens in determining use of sensors in public spaces. Use of sensors on infrastructure or with public services is likely to be less of an issue. Use of sensors in private spaces can be highly problematic and must comply with data privacy regulations, particularly HIPPA. The European Union's General Data Protection Regulation (GDPR) should also be considered as a standard for data privacy.

7.4 NEXT STEP TACTICS AND TASKS

To maximize efficient, effective use of sensors, the City of Chula Vista should:

- *Determine monitoring requirements based on municipal goals and departmental activities and initiatives*. Consider future scenarios such as fully autonomous vehicles, roving robots, etc.
    - Share those requirements openly and establish mechanisms for citizens to provide feedback on them.
    - Establish guidelines for gathering and publishing sensor data based on citizen input.
- *Develop municipal policies for sensors*, specifically related to access to city sensor network (i.e., which sensor can connect), data retention and sharing, use of standards (and level of openness/proprietary), etc.

[13] https://www.citylab.com/life/2017/04/singapore-city-of-sensors/523392/
[14] https://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf, page 22

- *Conceptualize full build out of sensor network and derive sensor requirements*, following local policies, and aligned with guidelines.
- *Prioritize build out based on strategic goals and imperatives*, focusing on establishing and evolving network infrastructure to support sensors.

8. Wi-Fi and Municipal Wireless Systems

The Scope of Work for this project includes analysis and evaluation of wireless infrastructure to provide municipal wireless systems for City use which are private and secure (Task 9) and a larger enterprise Wi-Fi infrastructure which is capable of supporting City operational needs and some level of access to the public (Task 4). The RFP suggests these tasks and subjects are related and Magellan agrees with that assessment. The integrated planning approach for municipal wireless systems needs expands to include targeted provision of Wi-Fi for public use as described below. Thus, we address the two tasks in this "Wi-Fi and Municipal Wireless Systems" section. The subject of Wireless Systems Security (Task 14) clearly relates to establishment of these municipal and public access systems, so we also address that important subject here. Similarly, wireless systems are key infrastructure for "Smart City" functions so we also address the import of wireless for Smart City applications here.

8.1 BACKGROUND

8.1.1 Wireless Technology Overview

> "Wireless is evolving, driven by more devices, more connections, and more bandwidth-hungry applications. Future networks will need more wireless capacity and reliability. That's where the sixth generation of Wi-Fi comes in."
>
> *Cisco Technical White Paper, IEEE 802.11ax: The Sixth Generation of Wi-Fi*

Cisco provides projections of internet growth and trends[15] including wired and wireless networks:

- More internet traffic will be created in 2022 that crossed global networks in the 32 years since the internet started.
- By 2022:
  - More than 28 billion devices will be connected to the internet.
  - Video will make up more than 80% of Internet traffic.
  - More than half of all devices and connections will be machine-to-machine, with an expected 14.6 billion connections, up from 6.1 billion.
- Average global Wi-Fi connection speeds will more than double to 54 Mbps.
- Growth in data traffic in North America will exceed 20% compound annual growth rate (CAGR).

[15] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1955935

Forecasts of mobile and Wi-Fi traffic by 2022[16] are a subset:

- Mobile traffic will represent 20% of total internet traffic.
- Smartphones will surpass 90% of mobile data traffic.
- 5G traffic will be more than ten percent of total mobile traffic.
- Nearly 60% of mobile traffic will be offloaded on to Wi-Fi.
- Nearly 80% of mobile traffic will be video.

Top mobile networking trends[17] include:

- The mix of wireless devices will evolve toward "smarter" mobile devices, including noticeable growth in M2M[18] devices, i.e., GPS systems in cars, asset tracking systems in shipping and manufacturing sectors, or medical applications making patient records and health status more readily available, and decline in non-smartphones and other portables.
- Cell network advances expanding 4G and implementing 5G, currently a 4G connection generates about three times more traffic than a 3G connection, and a 5G connection will generate about 3 times more traffic than a 4G connection.
- Continued growth (32% CAGR) of M2M connections (i.e., home and office security and automation, smart metering and utilities, maintenance, building automation, automotive, healthcare and consumer electronics) and emerging trend of wearable devices (worn on a person and have the capability to connect and communicate to the network either directly through embedded cellular connectivity or through another device – primarily a smartphone – using Wi-Fi, Bluetooth, or another technology).
- Wi-Fi's expanding role and coverage, offload from mobile wireless expected to be 59% of mobile traffic due to advanced devices attracted by 4G and 5G networks combined with data caps implemented by service providers.
- New mobile applications and requirements, mobile video growth of 55% CAGR will accelerate busy-hour traffic, Virtual Reality and Augmented Reality will proliferate and grow based on evolutions including 5G.

8.1.2 Wi-Fi versus Mobile Wireless

Mobile wireless communication occurs over a portion of the electromagnetic spectrum used for radio frequencies. The Federal Communications Commission manages and licenses these radio frequencies for mobile wireless use. Radio frequencies are divided into different bands that have different characteristics and are assigned different uses. For wireless networks these spectrum assignments can be characterized in three categories: low band (under 3 GHz) used primarily to connect mobile devices; mid-band (2 – 24 GHz) which provides a mix of coverage and capacity;

---

[16] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html#_Toc953325

[17] *Id*.

[18] Direct communication between devices using any communications channel, but in this case referring to wireless connections.

and high-band (above 24GHz) or millimeter wave spectrum which travels much shorter distances but provides much higher capacity and speeds and is being used for 5G.

In contrast to mobile wireless, Wi-Fi is a technology that allows an electronic device to exchange data or connect to the Internet wirelessly using radio waves (unlicensed spectrum) on a Wireless

> 5G is the next phase of mobile technology. 5G's primary improvements over 4G include high bandwidth (greater than 1 Gbps), broader coverage, and ultra-low latency. These features combined with enhanced power efficiency, cost optimization, high-precision positioning, massive IoT connection density and dynamic allocation of resources based on awareness of content, user, and location make 5G a flexible as well as transformative technology. 5G will be able to accommodate IoT applications such as sensors and meters at the low end of the of the IoT spectrum. But perhaps more importantly, it will also support autonomous cars and other tactile Internet driven applications such as augmented and virtual reality, factory automation (robotics), smart grid, et al. at the high end of the IoT spectrum.
>
> *Cisco White Paper, Global Mobile Data Traffic Forecast Update, 2017-2022; February 2019*

Local Area Network. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards" which range from 802.11b, the slowest standard, to 802.11ay, currently the fastest standard. Thus, Wi-Fi is the wireless version of a wired Ethernet network and in similar fashion connects computers and myriad other electronic devices to the network and to the Internet. Wi-Fi is provided by a wireless access point with a defined coverage area known as a "Wi-Fi hotspot" which can be configured to require authorization via password and other security levels. Increasing numbers of electronic devices – laptops, tablets, smartphones, security cameras, printers and scanners, home appliances, and myriad other devices support Wi-Fi connectivity.

"4G" mobile wireless communication is provided "everywhere" by national carriers using broad coverage from wireless towers and antennas, although connectivity can be poor or non-existent in certain buildings. 5G mobile wireless is an emerging standard designed to "fill in" 4G mobile wireless networking for capacity and speed purposes with smaller coverage areas. Wi-Fi on the

other hand is short range (50 to a couple hundred feet, unless used with Wi-Fi extender) and "local" using Wi-Fi hotspots/access points and wireless routers. The radio frequency is shared among users for both mobile wireless and Wi-Fi which affects transmission speeds provided to the users – the more users competing for the same transmission capacity, the slower the speed provided to individual users.

There is a common public misconception that "wireless service" is indeed fully wireless. In fact, typically the only "wireless" component to wireless service is the wireless transmission over radio spectrum between the user's cell phone and the cell tower (or Wi-Fi hotspot) at either or both ends of the call.[19] Wireless service places significant demands on the wireline network for connection of each cell tower or Wi-Fi hotspot to wireless providers' network facilities.

8.1.3 Wi-Fi

"Wi-Fi networks created a distributed connectivity fabric that enables Wi-Fi to carry the vast majority of wireless traffic and provide broadband connectivity where it is needed the most: in homes, inside buildings, and in dense outdoor areas. Wi-Fi has done this while making very efficient use of available unlicensed spectrum."[20]

[19] In some cases, operators have used radio spectrum to transmit consumer data and voice traffic from the transmitter on the tower to the base, where it is then connected to the landline network. But this engineering practice is going by the wayside as it consumes valuable radio spectrum and is otherwise less desirable from an engineering perspective, in favor of fiber connection of the transmitters on the tower to the base for connection to the landline network.

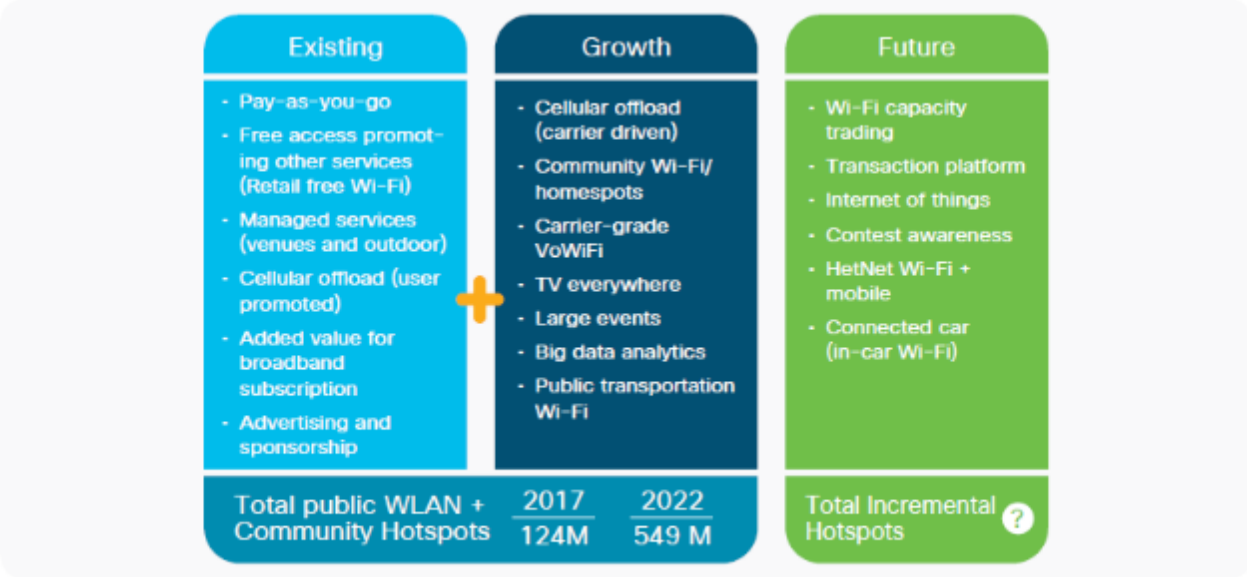
[20] "Next Generation Wi-Fi: The future of connectivity", the Wi-Fi Alliance, December 2018.

> Wi-Fi access has become synonymous with broadband access. Nearly all broadband homes have one Wi-Fi access point (AP) or a mesh Wi-Fi network. Cities provide free public Wi-Fi to deliver broadband access to their citizens to bridge the digital divide and provide services. It is virtually impossible to find an airport or a hotel that does not offer Wi-Fi access to visitors and guests. Within the home, Wi-Fi is the preferred connectivity method that goes beyond broadband connectivity to smartphones and laptops: most new smart home devices utilize only Wi-Fi and depend on it for setup, authentication, and operation.
>
> *"Next Generation Wi-Fi: The future of connectivity", the Wi-Fi Alliance, December 2018*

Key takeaways from the Wi-Fi Alliance report include:

- Next Generation Wi-Fi (Wi-Fi 6) and 5G are complementary technologies which expand the overall wireless connectivity fabric.
- Wi-Fi will continue to carry the bulk of the world's data traffic.
- Integration across multiple wireless access technologies enables seamless transition to cellular networks when outside Wi-Fi coverage areas.

Cisco reports public Wi-Fi hotspots are expected to grow four times on a global basis, with 26% CAGR growth expected in North America. Wi-Fi has evolved as a complementary network to offload data traffic from mobile wireless networks to lower cost Wi-Fi networks connecting to the internet.



Source: Maravedis, Cisco VNI Mobile, 2019

Figure 8-1 Global Wi-Fi Hotspot Strategy and 2017-2022 Forecast

Wi-Fi supports most "internet of things" (IoT) devices today which is fast-growing area of applications, including building monitoring, management and automation, smart home connectivity of sensors, thermostats, and security cameras, business applications in automation, manufacturing and monitoring, in-vehicle applications including wireless front and rear cameras and car remote diagnostics, and healthcare applications including patient monitoring. Wi-Fi also supports Smart Cities applications including automation of city services, linkage of sensors, cameras, parking meters and City staff mobile devices, and many other functions and capabilities.

Wi-Fi connectivity for the City for the variety of intended uses and purposes is strongly in line with, and supportive of, these wireless trends. Provision of Wi-Fi capability by the City will and can rely upon the proposed future City's core infrastructure including fiber network for connectivity and backhaul.

8.1.4 City of Chula Vista

As stated by the Telecommunications Master Plan RFP:

The City wishes to have a robust telecommunications infrastructure platform in order to further its goals of being a "Smart City", whereby significant cost savings, systems availability, and increased customer service can be achieved through the use of connective technologies to reduce power/water consumption, provide early warnings for systems which are experiencing technical issues, enhanced monitoring capabilities, remote sensing, providing public access to meaningful data (budget, public works projects, etc.) and deploy new and possibly unknown technologies in the future to further the City's Smart City endeavors.

Municipal Wi-Fi is a major component of the basic infrastructure needed to achieve "Smart City" goals. Municipal Wi-Fi needs fall into two immediate categories: Wi-Fi configured for use only by city employees and contractors; and Wi-Fi configured for use by the public at most but not all (e.g., Fire Department) City locations.[21] Opportunities exist for deployment of updated and upgraded Wi-Fi networking equipment in the City of Chula Vista. The cost of wireless network equipment has dropped significantly while the performance has improved dramatically. Determining where and how to build, deploy, and operate a fixed wireless broadband network is significantly less expensive and easier to manage than it was just a few years ago – and for a substantially better-performing network. Experience and technology/vendor improvements have smoothed out or otherwise addressed what were larger problem areas in early implementations, including practices to deal with frequency interference, balancing customer premise equipment deployment on the network, and software systems development to support network and operations administration.

The Magellan team was tasked to provide information and analysis which will take advantage of these trends and developments. This Plan is intended to support planning for a municipal wireless network which will provide demonstrable benefits to the community while meeting stakeholder needs, which is financially prudent while providing the greatest possible long-term benefits, and which clearly defines roles between the City and any private partners. The Magellan team worked with City leadership to schedule project meetings with individual City departments and their leaders. The meetings focused on discussion of departmental perspectives on the City's present telecommunications assets and environment as well as departmental visions of telecom requirements for future services and applications. City leadership also supported surveys completed by each City department regarding information and computer technology utilization at present, and what future needs are foreseen. These survey and interview responses have been very useful for the assessment contained here.

8.2 GENERAL REQUIREMENTS

The City seeks to determine the feasibility of upgrading present wireless systems and deploying a municipal wireless system providing secure data/voice capabilities for use by City employees and contractors at City locations, and further assessing the extent to which this infrastructure can be extended to support City or City contractor wireless devices in key public spaces and in addition provide public access on a separate portion of the network.

8.3 CURRENT SITUATION

Information Technology Services is responsible for overseeing and administering telecommunications for the City including the core network infrastructure and Wi-Fi capabilities. The City has significant deployment of Wi-Fi today including 120-130 access points. Today three

separate and different management consoles are used for Wi-Fi City-wide, which clearly limits the ability to manage Wi-Fi networking on a consolidated City-wide basis. Existing Wi-Fi equipment is generally "end-of-life" and thus ready for replacement. The City has no telecom budget line item at present.

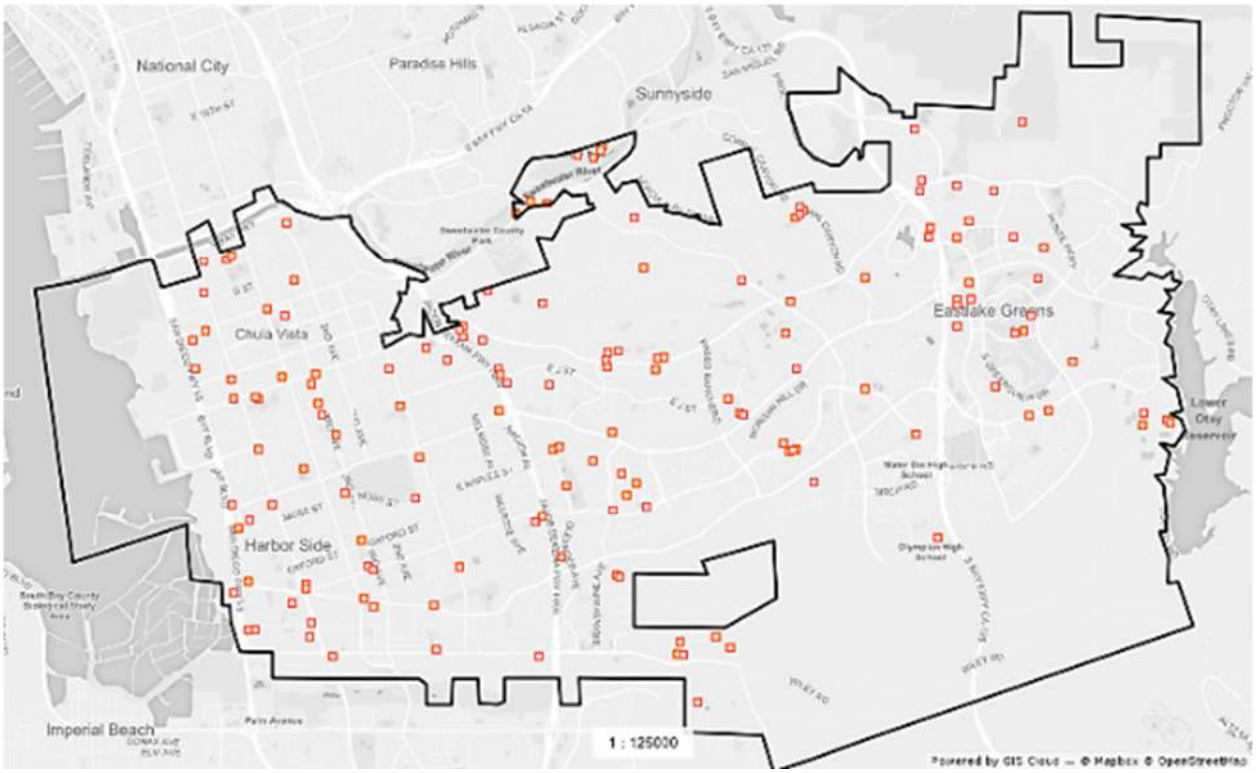


Figure 8-2 Current View of City of Chula Vista Wi-Fi Locations

The core network infrastructure consists of some fiber connecting City facilities and almost everything else on Cox Business Class Internet. Wi-Fi at present is considered to be "hodge-podge" as it has developed, with low throughput connection. City Wi-Fi generally provides for one guest and one City staff connection. There are large gaps in coverage at City Hall, which is particularly problematic in Council Chambers when there are large crowds. Other City sites can be worse. Looking forward, ITS sees the need for a unified, centrally controlled Wi-Fi network with high speed connections and thorough coverage in all City facilities. The City staff network would be secure and provide access to the enterprise network for City employees and contractors. An additional component of the network would be dedicated City-wide wireless networking for the primary use of City staff and transportation, with a segregated high-availability Wi-Fi for public safety and also the ability to segregate capacity so each facility has what it needs. City departments could use this network for remote sites such as irrigation controllers, and sensor networks established based on department needs. A secondary use could be free Wi-Fi access for the public.

Community Services Department includes Libraries, Parks and Recreation, Arts & Culture and related services. At present the libraries provide public Wi-Fi using Cox Cable connections and provides numerous online services such as business licensing, code violations, dog licensing, job opportunities and public safety careers, library services including catalog searches and reservation of library materials, city council meeting information, and registrations for classes and programs, among many other online services. The library also provides "MiFi hotspots" on a check-out basis to patrons for internet access using a T-Mobile data plan. Parks and Recreation currently maintains nine facilities[22] which offer free Wi-Fi. The Wi-Fi is useful for the public but also for city staff using computers to support on-site registrations for example. Public Wi-Fi is also provided in City parks for both staff and resident/guest use. But irrigation controllers use cellular wireless service (CDMA) at present rather than Wi-Fi. Better Wi-Fi would allow getting off old, expensive technology (e.g., 3G wireless). The City transition to expanded core networking and fiber placement (e.g., via the Traffic Signal Communications Master Plan) could enable a move to Wi-Fi support of these irrigation controllers and other functions. Also, there is a need for staff to be able to use tablets in the field for work management systems (provided by Lucity) and do documentation in the field. There are also various sensor and other applications using GPS, databases, etc. for park operations which are of interest looking forward.

At present the Community Services Department notes that Wi-Fi is open for the whole complex and seems to be "down" a bit from time to time as well as being "really slow". Looking forward the Department would like to have Wi-Fi coverage around all City properties and parks with a City employee secured Wi-Fi that is fast and available at all City locations, including libraries, recreation centers and parks, public works, fleet facilities, etc. Sensor networks need to be supported, particularly in parks, and digital signage and kiosks need to be supported for public use.

Public Safety needs were assessed by surveys and interviews with the Fire and Police Departments. At present the **Police Department** operates two SSIDs[23], one a secure network for law enforcement use and the other for public 'open' use by guests and employee personal devices. Looking forward, the Police Department would like three SSIDs – one for guests, one for employees, and the third for law enforcement systems. The Department visualizes a much broader use of wireless devices within and outside of the Police Department facility. Security and

[22] Heritage Recreation Center, Loma Verde Aquatic Center, Loma Verde Recreation Center, Norman Park Senior Center, Otay Recreation Center, Parkway Aquatic Center, Parkway Community Center, Salt Creek Recreation Center, and Veterans Recreation Center. Parks and Recreation operates five other facilities which do not have Wi-Fi service.

[23] Service Set Identifier, which is the primary name associated with an 802.11 wireless local network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks.

connectivity are key challenges for that vision, which implies tight integration with city infrastructure but logically separation via access controls and physical controls. The Police Department would also like to see infrastructure which supports sensor networking, which doesn't exist at present. This would include smart nodes with camera sensors on streetlights and PTZ[24] cameras where there is a lot of foot traffic (e.g., MTS stations, near schools, parks, major shopping centers and problem crime areas). The Department has a strong desire for smart nodes similar to deployments such as in San Diego using public safety video systems in the marketplace (e.g., totalrecallcorp.com). At present the **Fire Department** does not have City Wi-Fi at fire stations but obtains connectivity for union members using Cox Cable connections. Fire Department does desire to have secure City Wi-Fi deployed at the Fire Stations and administrative offices. Streaming video is important for observation at computer workstations and similar to consumer experience at home does not work well with slow or unreliable connections. (This need will be more pronounced with deployment of Next Generation 911.) Also, poor Wi-Fi connections impair interviews conducted over Skype connections. At present no sensor networks exists for Fire, but the Department (similar to the Police Department) desires to have smart nodes available with camera and weather sensors, and support for telemetry from fire apparatus, firefighters (medical monitoring), and medical instruments. Thermal cameras are important looking forward either on drones or on poles for wildland interface fire threats. Given the medical/EMT functions of the Fire Department secured Wi-Fi is a must to include and ensure HIPAA compliance.

The City recently completed creation of a City-wide **Traffic Signal Communications Master Plan**. The Plan includes bringing fiber optic connectivity and Cisco controllers to each traffic signal to support deployment of numerous Intelligent Transportation Systems devices for a more modern transportation system in the City. The type and sizing of switching is being explored with Power-over-Ethernet specified to support all data traffic via ethernet and also Wi-Fi access points. The Magellan team explored broader linkages to Smart City and Wi-Fi access points with departments and stakeholders. Fiber connectivity could potentially be used for backhauling for Wi-Fi coverage.

Similarly, the City is included with the SANDAG and CalTrans in participating with the U.S. Department of Transportation to operate one of ten proving grounds for autonomous vehicles, designated as an **Autonomous Vehicle Proving Ground**. Wireless technology is crucial for autonomous and connected vehicles.

The **Economic Development Department** at present desires stronger Wi-Fi signal to reach all offices and meeting rooms At present a permitting system (Acela) is used which relies upon wireless networks for data transmission and system access for supervisors and staff in the field. Coverage gaps require city staff to come back to the office for data entry. Economic Development foresees a number of applications and needs including dynamic and easy-to-understand signage

[24] Pan/Tilt/Zoom.

and other information, ability for field staff to use Wi-Fi with their phones, tablets, computers in their daily activities without having to come back to the office to do data entry, ability to communicate with units dispatched to a scene (drones, vehicles, etc.), kiosks to inform the public and facilitate interaction with the public, adequate bandwidth for transmission/access to plans and documents, and sensor networks for centralized monitoring and control of municipal assets.

The City is undertaking redevelopment of 535 acres of land on San Diego Bay in partnership with the San Diego Unified Port District, guided by the **Chula Vista Bayfront Master Plan**. Important features of the CVBMP include:

- Opening the Bayfront to new parks, open space, recreational amenities, and lower-impact future development.
- Development of new hotel and conference meeting space.
- New high-rise residential units.
- New office and retail spaces.
- Ultimately redeveloping the area to a mix of condominiums, retail shops, hotels, office and public open spaces.
- This will include advanced energy technologies and Smart City designs to incorporate cutting-edge technologies.
- Wi-Fi will be a crucial infrastructure need for this development.

The City has studied Bayfront development extensively including through a detailed assessment performed by Black and Veatch. The assessment laid out numerous offerings and possibilities, including basic infrastructure of connecting the Bayfront via fiber, using that fiber for backhaul to provide City and public Wi-Fi and information kiosks, public safety "smart nodes" and security cameras, parking guidance, information systems, crowd detection, leveraging the City's traffic signals and street lighting for Smart City and Wi-Fi purpose, and pedestrian/vehicle/bike counters. Further opportunities include smart irrigation, water quality monitoring, wildlife detection, waste pickup and route optimization. Finally, the City of San Diego has installed GE Smart Sensors, opening the possibility that the City could join and leverage that project.

Development of the **Millenia Urban Center** is also occurring in the eastern part of the City. "Millenia is planned for up to 3,000 multi-family residences, 2 million square feet of Class A office space on 30 acres, 1.5 million square feet of retail, hospitality, civic and mixed-use projects, six themed urban parks and a variety of tree-lined promenades, casual gathering places, bikeways, and plazas."[25] Wi-Fi will be a crucial infrastructure need for this development.

Other City departments also note that "Wi-Fi needs improvement" (e.g., Finance).

[25] RFP, page 4.

8.4 NEXT STEP TACTICS AND TASKS – WIRELESS IMPLEMENTATION STRATEGIES

Experience in other cities shows where wireless implementation strategies require decisions, including:

- What is the purpose of the wireless network?
  - Support City Functions
  - Address Public Access concerns
  - Address Digital Divide concerns
- What business model should be used?
  - Public Ownership and Operation, with or without other public or non-profit entities as partners
  - Public Ownership, with operations contracted through a service provider
  - Public-Private Partnership
- What is the source of funding?
  - City Budget
  - Grant or Partnership
  - Subscriber Fees
- What speed and capacity should the network provide?
  - Relatively low
  - Higher

8.4.1 Purpose of Wireless Network Implementation

Review of the information gathered from City staff managers and stakeholders indicates that there is a clear need to improve and extend Wi-Fi service to support City functions. Realizing the functions and opportunities of an improved and expanded Wi-Fi network can be achieved using a phased approach:

- Existing Wi-Fi equipment is "end-of-life" and suitable for replacement. This end-of-life status provides the opportunity to improve the network with an overall plan in mind (including backhaul via fiber-optic networking), which would:
  - Resolve the current "hodge-podge" nature of the network and improve coverage and speed at current Wi-Fi locations.
  - Implement centralized management and control of the City Wi-Fi network.
  - Add coverage at desired additional locations under the overall plan including desired high-speed fiber optic backhaul connectivity.
  - Support separation of secure City and guest networks and implementation of appropriate wireless system security.
- Consideration of expansion of City Wi-Fi networking to cover:
  - Existing gaps in network coverage.
  - Expanded use of digital devices (e.g., tablets) in the field by City staff and contractors in conjunction with permitting, GPS and database applications.
  - Sensor networks established based on department needs.

  - Management of controllers at remote sites, i.e., irrigation controllers.
  - Digital signage and wayfinding.
  - Operation of kiosks for public use.
  - Public Wi-Fi in City facilities and major parks and recreation centers.
  - Public safety applications including the "smart node" concept and technologies (e.g., telemetry applications, and camera and weather sensors) under appropriate security and governing policies.
- Consideration of expansion of City Wi-Fi networking beyond City locations to cover event spaces, strategic recreational and commercial districts and the like.
- Consideration of expansion of City Wi-Fi networking strategically placed through the City.

The information and analysis gathered in this project clearly suggest the City should plan to proceed with the first two phases. Whether to add the additional phases of expansion to event spaces and strategic recreational and commercial districts, or ultimately ubiquitous coverage of the City are separate decisions subject to additional study and planning considerations, including careful examination of incremental costs of expansion given the determination to upgrade and expand Wi-Fi coverage for City management and administrative purposes. Adding the latter two phases could also influence the City's choice of business model. It appears to the Magellan team from our interviews and stakeholder discussions that the City should plan to upgrade and expand the municipal Wi-Fi network to provide City employee/contractor secure Wi-Fi access via one or more SSIDs at City locations, major parks and recreation centers, locations specified by public safety agencies, and locations identified for kiosks, digital signage, sensors and controllers, and expanded use of digital devices in the field. An additional SSID would be established for public use on a City guest network.

8.4.2 Alternative Business Models

Under **Public Ownership and Operation**, the City manages all aspects of the wireless network. The City would own or procure the fiber optic networking necessary for backhaul and connectivity to the internet as well as the wireless equipment for the network and subsequent technology replacement costs. The City would be responsible for all construction costs, system operations and maintenance, customer service, digital inclusion initiatives, marketing and other functions. Requirements on the City for resources and technical skills is relatively high compared to other business models.

Under **Public Ownership and Contracted Operation**, certain functions are divided between the City and service providers to operate the wireless network. For example, the service provider handles the construction costs and wireless equipment costs and installation, while system operations and maintenance, customer service and marketing can be shared functions. Shared operations under contract lessen the demand on city resources and technical skills while reducing related risks.

A **Public-Private Partnership** (PPP, or P3) is a venture funded and operated through a collaborative partnership between a government and one or more private sector organizations. While details of the divisions of responsibilities between the public and private partner(s) can vary in general the wireless network is implemented and operated by the service provider with the City retaining ownership of infrastructure assets. Sharing under a P3 arrangement further lessens the demand on city resources and technical skills while reducing related risks.

Our interviews and stakeholder discussions have confirmed that a P3 or public ownership/contracted operation business model would be best suited to the City, rather than the public ownership business model. This is in line with the City's Smart City Vision through which Chula Vista has undertaken to work with various entities to further its Smart City goals, including but not limited to local/federal and state agencies, telecommunications providers, technology companies, and non-profit groups specializing in Smart City endeavors.

8.4.3 Funding and Risk

The different business models will have different funding requirements and revenue generation potential. Public ownership/operation has the highest funding requirements and financial risk, but any revenues garnered from the wireless operation inure to the City. These revenues are generally earned from wholesale and retail charges to users of the network. On the other end of the business model spectrum, under a P3 arrangement the City's financial risk is minimized and the revenue opportunity for the City is "capped" consisting perhaps of fees paid by the private partner for use of the City's assets and infrastructure, while the private partner earns the wholesale and retail revenues by dint of sales, marketing and operational effort. The public ownership/contracted operation falls in the middle of the spectrum established by these two end points.

8.4.4 Network Speed and Capacity

The City will need to consider various trade-offs in its decision, including determining what speed and capacity to implement in its municipal Wi-Fi network. New technologies make higher speeds achievable but there are cost and technical implications from implementing these higher speeds.

8.4.5 Tasks and Recommendations

It is clear from surveys and information gained from stakeholder meetings and departmental perspectives that there are documented needs for upgrading and expanding the City's Wi-Fi footprint and capacity. This expanded City Wi-Fi network would be intended to support City staff and contractors in performance of their duties and the public need for information while on the premises of City locations and major parks and recreation centers. This platform could be expanded to City-wide coverage at a later date if indicated by future planning. The success of this wireless strategy will depend on other investments in City fiber and other broadband infrastructure as described throughout this Plan under a long-term integrated planning process. Many supporting parts are being implemented through the traffic signal upgrade process, connection of streetlights to fiber facilities, and Bayfront planning processes and the City's "Smart

City" vision. Upgrade and expansion of the Wi-Fi network will contribute to the Smart City visions of a network which:

- Connects all City facilities with secure, cost-effective, redundant and flexible network infrastructure.
- Enables the City to meet aggressive energy savings requirements associated with Bayfront development plans
- Facilitates innovation and economic development
- Supports provision of timely and accurate data to centralized processing locations from a myriad of sources including IoT devices, mobile units and other infrastructure
- Connects citizens to City services and provides access to connect citizens to their government.

The City should support the expanded Wi-Fi network through an RFP process to select a service provider to upgrade and operate the Wi-Fi network, or work to identify and select a private partner in formation of a Public-Private Partnership to provide Wi-Fi networking.

Further detailed planning internal to the City is needed to determine:

- The time period (multi-year) over which the Wi-Fi network upgrade and expansion is to be accomplished, balancing financial and technical requirements vs. City needs.
- The phasing and prioritization of locations for installation of equipment and turning up Wi-Fi service.
  - Specific City facility locations
  - Specific parks and recreation center locations
  - Bayfront, Millenia Urban Center and other locations
  - Other corridors or locations to be determined
- Requirements associated with extending the network to accommodate guest access and separate SSIDs.
- Any necessary data center requirements associated with the upgraded and expanded Wi-Fi network.
- Fiber optic cable requirements for backhaul to support these locations and phased deployment. Backhaul options need to be identified and planned to ensure adequate capacity in operation.

Once the City has determined locations, location priority and phasing the City should issue a Request for Proposals for a service provider to install, operate and manage the Wi-Fi network. The service provider will need to conduct a Wi-Fi Planning and Site Survey assessment to provide the analysis needed to design, verify and troubleshoot the City's Wi-Fi network. This Assessment should include performing a RF spectrum analysis (2.4 and 5 GHz), an automatic coverage and signal quality study of all existing access points and identifying key points to improve the performance of voice and data communications and include Wi-Fi Heat maps providing the City with a graphic illustration of the RF distribution footprint for its wireless 802.11xx coverage. This

assessment would provide the information needed to plan a secure, fast and reliable network design to ensure the best placement of wireless access points for adequate coverage.

9. Operations & Maintenance Costs

Magellan examined the current list of IT projects to assess the personnel needs for Information and Technology Services (ITS). As of Jan 2019, ITS had thirteen (13) staff under the leadership of IT Director Ed Chew. In addition, four (4) staff are detailed to Police Department with a dotted-line reporting responsibility back to Mr. Chew, to ensure consistent direction of infrastructure is utilized throughout the City.

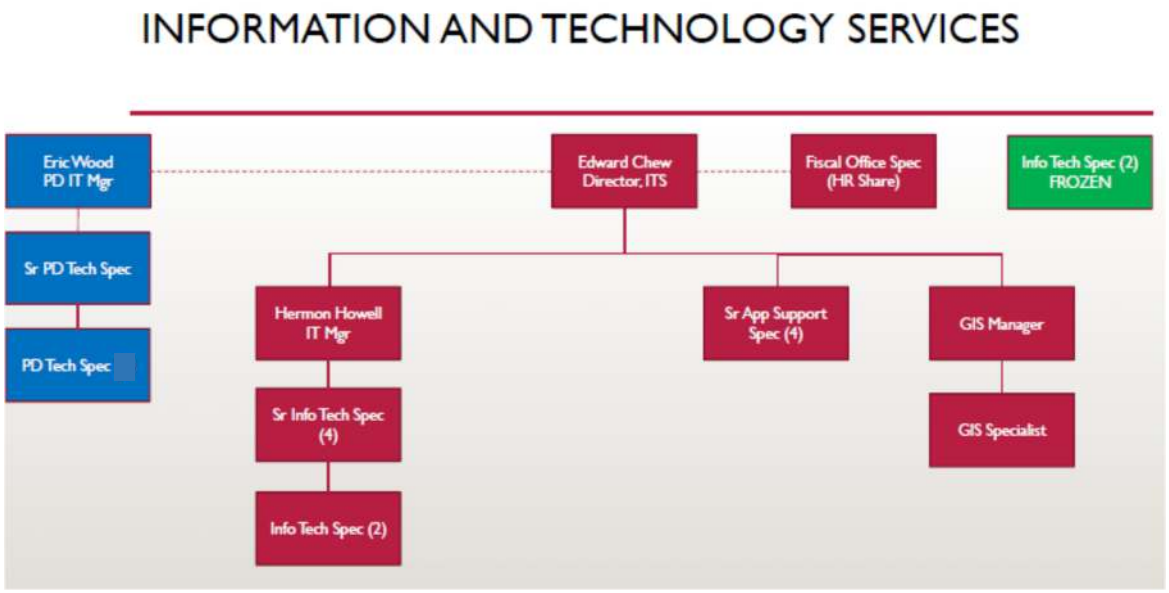


Figure 9-1 Information and Technology Services Organizational Chart

9.1 PROJECTS LIST

As of November 2019, current ITS projects list includes the following:

1. Network Migration
2. Wi-Fi Migration
3. Exchange Online
4. Domain Consolidation
5. Automate Routine, Low-Value Tasks
6. PKI Implementation
7. Telephony Overhaul
8. SharePoint Migration
9. Microsoft (?) Teams Deployment
10. Electronic Forms Routing, Workflow
11. Azure Migration
12. eDiscovery
13. Single Signon and Federated Access

14. Mobile Device Management
15. Computer Aided Dispatch (CAD) Upgrade
16. Police – MDC Replacement, Smartphone Replacement
17. Security Cameras
18. GIS Upgrade
19. Traffic Upgrades
20. Microsoft Annual True-Ups and License Management

9.2 ADDITIONAL STAFF RECOMMENDATIONS

Magellan recognizes that budgets are limited in Chula Vista. Magellan also realizes there are many years of work in the above project list. As a result, Magellan recommends the addition of 1 Senior Engineer ($90K) and 1 Project Manager ($90K).

10. Long Term Costs

This section summarizes the capital costs of constructing the fiber network described in Section 2.

10.1 FIBER NETWORK METRICS BY IMPLEMENTATION PHASE

There are no revenues associated with this fiber model, as the network will only be used by Chula Vista City Government and affiliated entities. Cost reductions can only be achieved by displacing current commercial telecommunications costs.

Reiterating, the following table summarizes the metrics by ring, by phase.

		Core / Backbone		Laterals / Distribution		Core + Laterals	
Ring	Phase	Linear feet	Linear miles	Linear feet	Linear miles	Linear feet	Linear miles
1	1	73,371	13.90	2,539	0.48	75,910	14.38
1	2		0.00	112,855	21.37	112,855	21.37
1	3		0.00	35,953	6.81	35,953	6.81
2	4	70,343	13.32	31,332	5.93	101,675	19.26
2	5		0.00	81,280	15.39	81,280	15.39
3	6	32,953	6.24	17,971	3.40	50,924	9.64
		176,667	33.46	281,930	53.40	458,597	86.86
		38.52%		61.48%			

Figure 10-1 Summary of Fiber Network Metrics, by Ring, by Phase

10.2 POSSIBLE COSTS BY IMPLEMENTATION PHASE

All Magellan recommendations for the implementation of Chula Vista's fiber network are entirely wired solutions; there are no recommendations for any wireless last-mile technologies to City buildings as part of the program. Construction of all backbone and all lateral connections are recommended to be underground and all services provided by the P3 will utilize those assets. No wireless assets are included in this plan for any last-mile service delivery.

These construction cost estimates include expected prevailing wage considerations. The City of Chula Vista should consult with its Attorneys and Counsel to determine if prevailing wages would apply.

If prevailing wage does apply to any construction costs, the City should review State of California's Department of Industrial Relations (DIR) Prevailing Wage sheets for County of Ventura to determine appropriate rates. Current Wage Determination is 2019-2, as of this writing.

If any federal funds are used, say for transportation projects upgrading twisted wire pair, there may be additional prevailing wage considerations related to compliance with Davis-Bacon Act.

Magellan assumed each ring was implemented in a single year, starting in three successive years. Therefore, total duration on the project would be three years, starting in fiscal year 2021.

Magellan constructed a cost estimate by phase, including these costs in a subset of its Broadband Financial Sustainability ("BFS") Model. The cost estimates, by ring and by phase, are estimated at $18.73 million, which includes a 10% contingency. Details are provided in the following figure.

	Phase	Linear feet	Pctg	Linear miles	Labor	Materials	Contingency	Des/Eng
Ring 1 (Req)	1	224,718	49.00%	42.56	7,043,385	873,076	791,646	238,073
	2							
	3							
Ring 2 (Cont)	4	182,955	39.89%	34.65	5,706,011	951,744	665,776	228,248
	5							
Ring 3 (Cont)	6	50,924	11.10%	9.64	1,628,368	304,569	193,294	106,925
		458,597	100.00%	86.86	$14,377,765	$2,129,389	$1,650,715	573,246
						$16,507,154	$18,157,869	$18,731,116

Figure 10-2 Summary of Fiber Network Construction Costs, by Ring, by Phase

10.3 POSSIBLE SAVINGS RELATED TO FIBER NETWORK

Under the proposed fiber network plan, as the network is planned to be used for internal operational and efficiency purposes, there are no direct revenues from outside sources provided to Chula Vista. Direct cost savings will be realized when there is a replacement for the current commercial communications offerings provided by Cox Communications and by AT&T.

As of October 2019, actual annual communications spending by Chula Vista with AT&T are approximately $218K, and with Cox Communications are approximately $149K, for a total spend of just under $370K annually.

ATT:	217,209.72
Cox:	148,862.52
Combined Spend	**366,072.24**

Figure 10-3 Current Annual Communications Spending

For simple analysis purposes, Magellan assumed that all external communications spending can be eliminated once the network is complete. There will likely be some residual spending. However, making that assumption, measuring capital investment on construction costs against operational savings puts the breakeven point at much longer than 40 years. This fiber network investment is simply not economically feasible on a financial basis alone.

Once the fiber network is operational, there may be some second-order revenues earned indirectly through wireless attachment fees (e.g. 5G wireless attachments); these are considered indirect revenues.

10.4 CHULA VISTA FINANCIAL SUMMARIES ON NETWORK BUILD

Magellan's analysis suggests that the phased construction of the three rings, in six phases, comes to an estimated total cost of $19.4 million. Costs are broken out as follows:

- Labor and Materials: $16.507 million
- Contingency on L&M: $1.651 million, at 10%
- Design and Engineering: $573K
- Construction Management" $480K over three construction waves
- Project Management: $384K over three construction waves
- Equipment and Electronics: $435K, including 20% for installation services

Ring	Phase(s)	Sites	Labor & Material	10% Contingency	Design and Engineering	Total Const, Des & Eng	Const Mgt	Project Mgt	Equipment *	Total
1 (Req)	1,2,3	20	7,916,462	791,646	238,073	8,946,181	180,000	144,000	283,010	**9,553,191**
2 (Cont)	4,5	7	6,657,756	665,776	228,248	7,551,779	180,000	144,000	87,080	**7,962,859**
3 (Cont)	6	0	1,932,937	193,294	106,925	2,233,156	120,000	96,000	65,310	**2,514,466**
		Totals:	**16,507,154**	**1,650,715**	**573,246**	**18,731,116**	**480,000**	**384,000**	**435,400**	**20,030,516**
			* = Includes professional services for installation							
			(Req = Required; Cont = Contingent on Funding)							

Figure 10-4 Financial Summary for Network Build

10.5 CHULA VISTA FINANCIAL SUMMARIES ON NETWORK BUILD

Magellan estimated the three waves of construction would be implemented in three years, starting in 2021 – 2022 (fiscal 2022), with each wave taking one year. City of Chula Vista may choose to lengthen construction time estimates, or stagger waves beginning two or three years after start of each wave. Total expenditures would likely remain unchanged, but funding considerations may be affected.

The models do not assume any savings realized by the City of Chula Vista for using its own network, in lieu of using a for-profit provider, to connect their own facilities.

Financing assumptions for Chula Vista financial analysis are as follows:

- Standard straight-line depreciation rates are used
- All construction and operating funds will be borrowed
- Loan term – 20 years
- Payments – steady monthly installments
- Interest rates – 3.50% fixed rate

Complete sets of the following graphs may be found in **Appendix D, "Financial Analysis for Chula Vista":**

- EBITDA and Net Income ($ millions)
- Cumulative Unrestricted Free Cash Flow ($ millions)
- Debt Balance ($ millions)
- Annual Unrestricted Free Cash Flow ($ millions)

- Annual Capital Spending ($ millions)

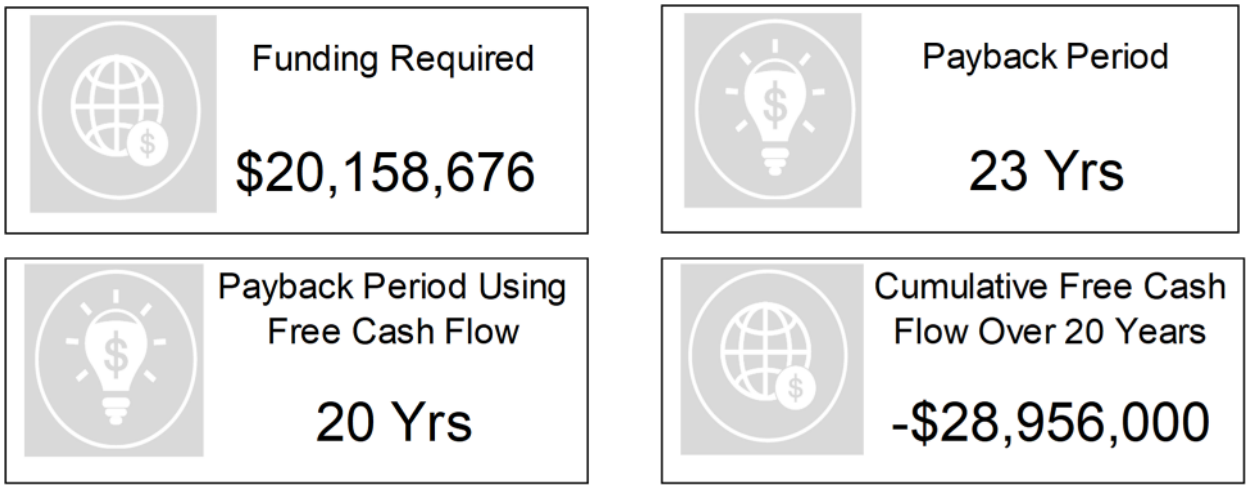


Figure 10-5 Financial Summary

11. Current Environment (Suitability for Smart Cities)

11.1 MINIMUM REQUIREMENTS FOR SMART CITIES SUPPORT

The City of Chula Vista must achieve a minimum set of objectives to provide support for Smart City activities within Information and Technology Services (ITS). Among these are:

- Fiber Network – Citywide and robust enough to provide backhaul for 5G and other smart city enabling devices, enabling smart applications. A fiber network is essential to support Smart Cities. Whether Chula Vista intends to build its own network or create a public-private partnership with other third-party entities, fiber network operation is both necessary and critical to providing backhaul to data collected with 5G and Smart City devices. In addition, device control and transmission of data to 5G device attachments requires fiber. See Section 2, "Core Infrastructure and LAN/MAN Opportunities" for detail on the proposed fiber network.
- Policies – To support governance and appropriate use of data to manage these Smart City applications. Data collected by 5G Smart City devices is critical. 5G devices will capture large amounts of data. In order to fully become a Smart City, however, decisions must be based on these large datasets. Significant investment must be made in policies and supporting operational systems. See Section 12, "Data Policies" for complete detail on the key five policies required.
- Appropriate Pricing – For Smart City attachments offered by wireless and other communications carriers. Price setting for Smart City and wireless 5G attachments is another critical component. Chula Vista should review its current pricing and confirm that $270 per pole (or municipal asset) attachment is sufficient. See Section 15, "Valuation of City Assets" for guidance on setting fees and prices.
- Additional Staffing – With ITS relatively short-staffed given the projects list outlined in Section 9.1, additional engineering and project management staff must be added to provide support for Smart City initiatives. Staffing augmentation contracts and contractors may provide specific technical skills but will require additional funding.

In summary, with the implementation of the fiber network, the development of policies and setting proper price valuations for connecting 5G devices assets, Chula Vista is poised to participate in Smart City planning.

11.2 ITS SWOT ANALYSIS

In competitive, non-monopolistic situations, organizations frequently assess their capabilities through a SWOT analysis. This analysis assesses the Strengths (S), Weaknesses (W), Opportunities (O), and Threats (T) which confront the organization in fulfilling its mission, strengthening its brand, increasing its market share, or improving its performance.

City of Chula Vista ITS is an internal, monopoly supplier of technology services. As such, it is the default provider of technology infrastructure for the City; there are no natural competitors or impediments to ITS executing its role within the City. However, there is some applicability in performing SWOT. Magellan assesses ITS as follows:

11.2.1 Strengths

- Trust – ITS Director Ed Chew is trusted by City Manager, City Administration. Mr. Chew has long, successful tenure with the City, having filled key technology support and leadership roles within the Police Department. Having served effectively, Mr. Chew was asked to assume management responsibility of ITS, bringing trusted management and leadership to ITS.
- Key Persons – There are several key individuals with detailed technical and operational knowledge (e.g. H. Howell is particularly critical).

11.2.2 Weaknesses

- Operating Budget – ITS has a very finite budget insufficient to adequately address new programs and project initiatives.
- Staffing – As of January 2019, ITS had a staff of thirteen (13) full-time employees and contractors, along with an additional four (4) staff detailed to Police Department. GIS staff are not included in these counts.
- Over-Utilization of Current Resources – There is insufficient slack time to invest in providing training in new technologies for high-value employees, and even to work on new project and program initiatives.

11.2.3 Opportunities

- Operating Budget Increases – Subject to fiscal realities within the City, ITS has the opportunity to augment its staff with key technical subject matter experts to support Smart Cities, Cisco DNA, software-defined networks (SDN), and other strategic improvements.
- Migration to Cloud – With more applications moving to the cloud, including enterprise resource management (ERM) systems, opportunities to improve leverage ratio of support staff to applications.

11.2.4 Threats

- Council Commitments - Political and Optics Risks – Without committed capital funding, Council, City Management and ITS would be exposed to commitments made to construct this fiber network.
- Third-Party Technology Providers Procured Outside of ITS – ITS has opportunity to review all technology procurements. Other departments with larger budgets might choose to look elsewhere besides ITS for support of initiatives.

11.3 ITS STAFF RECOMMENDATIONS

As of November 2019, there are at least twenty (20) significant projects on the ITS projects list, many of which focus on operational improvements and security, and not strategic initiatives. The projects list is included in this section.

Magellan recognizes that budgets are limited in Chula Vista. Magellan also realizes there are many years of work in the above project list. However, Magellan recommends the addition of one (1) Senior Engineer ($150-170K) and one (1) Senior IT Specialist ($135-$150K) to work on project backlog and support design of Smart City initiatives. Project Management improvements are necessary, to increase project capacity, standardize project execution, and provide consistent status reporting to senior management; Magellan recommends one (1) Project Manager ($140-160K). Finally, with cyber-security concerns ever-present and increasing, Magellan recommends creation of a Chief Information Security Officer ("CISO") role ($150-$175K). (All position estimates are fully loaded, including 30% benefits.)

12. Data Policies

12.1 BACKGROUND

City of Chula Vista should review, finalize and implement the five data policies detailed at the end of this section. These policies include:

- Data Privacy Policy – Governs and describes what City data is to be protected and why.
- Open Data Policy – Governs and describes what City data is shared with whom for which purposes.
- Data Ownership Policy – Governs and describes responsibilities of owners of data sets and provides guidance on framework for determining appropriate use.
- Smart Cities Readiness Policy – Governs and describes enabling governance and actions to support Smart Cities.
- Dig Once Policy – governs and describes how new conduit and fiber may be laid within City to minimize disruption to public right of way while maximizing participation of City, utility and private entities in installing new assets.

It is important to recognize that the draft policies included in this report represent one starting point for City's internal review, the output of which will be a policy for approval by City Management and City Council, if appropriate.

12.2 GENERAL REQUIREMENTS

City of Chula Vista has its own policy development process which collects input from all key stakeholder departments; is reviewed by Finance, Law, Human Resources and other departments; and is ultimately reviewed and approved by City Management and City Council.

As each of the five policies is finalized, City of Chula Vista should consider these additional factors in defining policy and in developing procedure and operational controls.

- Secure Access Control – How to ensure that only approved individuals with specific role capabilities have proper access to network, systems, application capabilities, and technology.
    - Security and Authentication – How to confirm that individuals authenticate to specific applications. This may entail implementation of two-factor authentication, which typically requires physical and knowledge information. Physical information may be possession of a device which identifies the individual (and may even be biometric, such as a thumbprint) and possession of information (such as a password). Public Key Infrastructure (PKI) guidance may be helpful in designing two-factor authentication methods.
    - User ID Management – Active management of user ids by system owners. This may also include delivery of login credentials via one method, and password delivered out of band to the login credentials.

  - Data Encryption – Consider appropriate levels of data encryption and secure internet protocols for application operation.
  - Remote Access – Consider establishing additional secure identification for remote access into network and into applications.
- Privacy and Confidentiality – Considerations of privacy of data, coupled with confidentiality and non-disclosure, must be considered.
- Data Management Considerations
  - Data Retention and Data Destruction – Policies must be developed with consideration of how long specific data must be maintained and, as important, when specific data must be deleted irrecoverably.
  - Backup and Recovery Processes – Policies and processes to be developed to ensure current backups are always available and can be efficiently and quickly restored in a response to a request, legal, operational, or otherwise.
  - Disaster Recovery and Business Continuity – Policies for systemic backups to support disaster recovery operations, should the data center or a specific location be disrupted, short-term. More significant, business continuity policies, operations, and plans should be developed in the event long-term access to key City operational locations is precluded.
  - Public Records – Policies must support public records requests, reliably and efficiently.
- Application Considerations
  - Business Information (BI) Systems and Processes – Considerations of key financial, transactional and government systems must be evaluated in context of ability to provide business information and analysis efficiently and timely. Flexibility is key, permitting access to any key systems to provide decision support to management and Council.
  - Systems Interfaces, Integration Planning and Architecture (also, Extraction, Transformation and Loading (ETL) Data Processes) – Policies should address who defines which data can be shared, with whom, and under what conditions. These may be regular production interfaces or extracts to data repositories or warehouses.
  - Mobile Operations – Policies should address how applications and data will be accessed remotely via secure devices. Need to avoid coming "home" to base operations to access applications and data is critical.
- Infrastructure Considerations
  - Operating System Patches – Policies should ensure that operating systems updates, patches, and security updates are consistently and timely applied. Supporting procedures must be defined and implemented.
  - Anti-Virus and Malware Software - Policies should ensure that anti-virus and malware updates are consistently and timely applied. Supporting procedures must be defined and implemented.
  - Architecture and Integration Planning – Policies should enable the development and implementation of an overall application enterprise architecture, along with plans for reliable integration of data streams, whether in real-time or in overnight batches.
- Enterprise Applications

- E-mail – Policies should support Office 365 implementation and operation, including guidance on sharing, managed group access to specific mailboxes, uses of mailboxes assigned to functions rather than to individuals, etc.
- GIS Applications – Policies governing what data is appropriate for storage in GIS applications. These should guide how decisions are made on which data is to be incorporated.
- Web Infrastructure – Policies on web design, operation, decentralized management must be developed and implemented.

- Cloud vs On Premise Operations – Policies need to consider whether data is based in cloud or is hosted on premises. Sufficient bandwidth is always a consideration as migration to cloud or software-as-service applications continues.

12.3 GOVERNANCE & POLICIES

12.3.1 Data Privacy Policy

Introduction

The Data Privacy Policy emphasizes the City's efforts to protect the personal information collected from the public. It should serve as a guide for all City departments that collect and use personal information in the course of conducting business.

Definitions

Data: For the purposes of this Policy, the term "data" refers to all structured information, unless otherwise noted.

Dataset: For the purposes of this Policy, the term "dataset" refers to a collection of data presented in tabular or non-tabular form.

Government information: "Government information" means information created, collected, processed, disseminated, or disposed of, by or for Chula Vista.

Information: "Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information life cycle: "Information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Personally identifiable information (PII): "Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available (in any medium and from any source) that, when combined with other available information, could be used to identify an individual.

Scope

The Privacy Policy applies to the collection, use, disclosure, sharing and retention of personal information obtained from individuals interacting with City departments, whether in person, on a website, or by mail in the course of providing City services. Each City department will strive to abide by and use this Privacy Statement to direct the handling of personal information, though from time to time it may be necessary for a City department to develop a practice that differs from this Policy.

The policy may not apply to personal information obtained by the City of Chula Vista in its capacity as an employer. The Human Resources Department should be consulted further on this matter.

Policy Requirements

Sections should include:

- Privacy Principles
- Privacy Policy Statement
  - Purpose
  - Scope
  - Data Classes
  - Opt-out
  - Use of Information
  - Data Retention
  - Accuracy
  - Accountability
  - Equity
  - Others as the City sees fit

Implementation

1. Determine a publicly available Purpose Statement that addresses the goals and guiding principles for the Policy. The Statement should be representative of and agreed upon by all City departments, including City leadership.
2. Specify the scope of the policy to cover all departments and all personal information gathered, with an exception for Human Resources information and/or other classes of data as specified by Human Resources, City Attorney, and others.
3. Enumerate classes of data and their sources. The City should consider all applications in use, records and permitting, demographics, and visitors to the City's website. Identify an owner for each class of data, who is responsible for recommending and enforcing privacy policy as determined by the City.
4. Develop a draft data policy. Magellan recommends that the City start with a framework created from a policy recently enacted and used in another City. The City of Seattle's policy would serve as a good start point and can be found at https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#x58255

5. Create a review process. Magellan recommends that the City review the Data Privacy Policy at least annually. The review should include modifications to the current policy, as well as adding any new data classes. The process creation should also specifically identify who will participate in this review.
6. Policy approval process, as required by the City of Chula Vista. This will include a review by the City Attorney, departments, Privacy Working Group and approval and acceptance by City leadership.
7. Publish the policy on the City's website, where it is easily accessible to the public. The City may also choose to provide some additional links such as Frequently Asked Questions (FAQs) and/or statements from City leadership concerning privacy.

12.3.2 Open Data Policy

This document is provided to City of Chula Vista, CA, as a set of recommended inputs and guidance which may form the basis for a formal Policy.

Introduction

Information is a valuable resource and a strategic asset to the City of Chula Vista Government ("Chula Vista"), its partners, and the public. In order to ensure that Chula Vista is taking full advantage of its information resources, departments and agencies (hereafter referred to as "agencies") must manage information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information. Managing government information as an asset will increase operational efficiencies, reduce costs, improve services, support mission needs, safeguard personal information, and increase public access to valuable government information.

Making information resources accessible, discoverable, and usable by the public can help fuel entrepreneurship, and innovation. This Policy establishes a framework to help document the principles of effective information management at each stage of the information life cycle to promote interoperability and openness. Whether or not particular information can be made public, agencies can apply this framework to all information resources to promote efficiency and produce value.

This Policy requires agencies to collect or create information in a way that supports downstream information processing and dissemination activities. This includes using machine-readable and open formats, data standards, and metadata for all new information creation and collection efforts. It also includes agencies ensuring proper information stewardship through review of information for privacy, confidentiality, security, or other restrictions to release. Additionally, it involves agencies building or modernizing information systems in a way that maximizes interoperability and information accessibility, maintains internal and external data asset inventories, enhances information safeguards, and clarifies information management responsibilities.

Definitions

Data: For the purposes of this Policy, the term "data" refers to all structured information, unless otherwise noted.

Dataset: For the purposes of this Policy, the term "dataset" refers to a collection of data presented in tabular or non-tabular form.

Government information: "Government information" means information created, collected, processed, disseminated, or disposed of, by or for Chula Vista.

Information: "Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information life cycle: "Information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Personally identifiable information (PII): "Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available (in any medium and from any source) that, when combined with other available information, could be used to identify an individual.

Open data: For the purposes of this Policy, the term "open data" refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users. In general, open data will be consistent with the following principles:

- *Public*. Agencies must adopt a presumption in favor of openness to the extent permitted by law and subject to privacy, confidentiality, security, or other valid restrictions.
- *Accessible*. Open data are made available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed, and searched. Formats should be machine-readable (i.e., data are reasonably structured to allow automated processing). Open data structures do not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes, often by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.

- *Described*. Open data are described fully so that consumers of the data have sufficient information to understand analytical limitations, security requirements of data, as well as how to process the data. This involves the use of metadata (i.e., fields or elements that describe data), thorough documentation of data elements, data dictionaries, and, if applicable, additional descriptions of the purpose of the collection, the population of interest, the characteristics of the sample, and the method of data collection.
- *Reusable*. Open data are made available under an open license that places no restrictions on their use.
- *Complete*. Open data are published in primary forms (i.e., as collected at the source), with the finest possible level of granularity that is practicable and permitted by law and other requirements. Derived or aggregate open data should also be published but must reference the primary data.
- *Timely*. Open data are made available as quickly as necessary to preserve the value of the data. Frequency of release should account for key audiences and downstream needs.
- *Managed Post-Release*. A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements.

Scope

The requirements of this Policy apply to all new information collection, creation, and system development efforts as well as major modernization projects that update or re-design existing information systems. The requirements apply to management of all datasets used in an agency's information systems. Agencies are also encouraged to improve the discoverability and usability of existing datasets by making them "open" using the methods outlined in this Policy, prioritizing those that have already been released to the public or otherwise deemed high-value or high-demand through engagement with customers. Agencies should exercise judgment before publicly distributing data residing in an existing system by weighing the value of openness against the cost of making those data public.

Policy Requirements

Agencies management of information resources must begin at the earliest stages of the planning process, well before information is collected or created. Early strategic planning will allow Chula Vista to design systems and develop processes that unlock the full value of the information and provide a foundation on which agencies can continue to manage information throughout its life cycle.

Agencies shall take the following actions to improve the management of information resources throughout the information's life cycle and reinforce the government's presumption in favor of openness:

1. Collect or create information in a way that supports downstream information processing and dissemination activities

Agencies must consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle. Accordingly, to the extent permitted by law, agencies must design *new* information collection and creation efforts so that the information collected or

created supports downstream interoperability between information systems and dissemination of information to the public, as appropriate, without the need for costly retrofitting. This includes consideration and consultation of key target audiences for the information when determining format, frequency of update, and other information management decisions. Specifically, agencies must incorporate the following requirements into future information collection and creation efforts:

1. Use machine-readable and open formats - Agencies must use machine-readable and open formats for information as it is collected or created. While information should be collected electronically by default, machine-readable and open formats must be used in conjunction with both electronic and telephone or paper-based information collection efforts. Additionally, in consultation with the best practices found in Project Open Data and to the extent permitted by law, agencies should prioritize the use of open formats that are non-proprietary, publicly available, and that place no restrictions upon their use.
2. Use data standards - Consistent with existing policies relating to agencies' use of standards for information as it is collected or created, agencies must use standards in order to promote data interoperability and openness.
3. Ensure information stewardship by using open licenses - Agencies must apply open licenses to information as it is collected or created so that if data are made public there are no restrictions on copying, publishing, distributing, transmitting, adapting, or otherwise using the information for non-commercial or for commercial purposes. When information is acquired or accessed by an agency through performance of a contract, appropriate existing clauses shall be utilized to meet these objectives while recognizing that contractors may have proprietary interests in such information, and that protection of such information may be necessary to encourage qualified contractors to participate in and apply innovative concepts to government programs.
4. Use extensible metadata - Agencies must describe information using metadata in consultation with the best practices as it is collected and created. Metadata should also include information about origin, linked data, geographic location, time series continuations, data quality, and other relevant indices that reveal relationships between datasets and allow the public to determine the fitness of the data source. Agencies may expand upon the basic metadata based on standards, specifications, or formats developed within different communities (e.g., financial, health, geospatial, law enforcement). Groups that develop and promulgate these metadata specifications must review them for compliance with the common core metadata standard, specifications, and formats.

2. Build information systems to support interoperability and information accessibility

Through their acquisition and technology management processes, agencies must build or modernize information systems in a way that maximizes interoperability and information accessibility, to the extent practicable and permitted by law. Agencies must exercise forethought when architecting, building, or substantially modifying an information system to facilitate public distribution, where appropriate. In addition, the agency's CIO must validate that the following minimum requirements have been incorporated into acquisition planning documents and

technical design for all new information systems and those preparing for modernization, as appropriate:

- The system design must be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design. In general, this will involve the use of standards and specifications in the system design that promote industry best practices for information sharing, and separation of data from the application layer to maximize data reuse opportunities and incorporation of future application or technology capabilities.
- All data outputs associated with the system must meet the requirements described in part IV of this Policy and be accounted for in the data inventory; and
- Data schema and dictionaries have been documented and shared with internal partners and the public, as applicable.

3. Strengthen data management and release practices

To ensure that agency data assets are managed and maintained throughout their life cycle, agencies must adopt effective data asset portfolio management approaches. Within one (1) year of the date of this Policy, agencies and inter-agency groups must review and, where appropriate, revise existing policies and procedures to strengthen their data management and release practices to ensure consistency with the requirements in this Policy, and take the following actions:

1. Create and maintain an enterprise data inventory - Agencies must update their inventory of agency information resources to include an enterprise data inventory, if it does not already exist, that accounts for datasets used in the agency's information systems.
2. Create and maintain a public data listing - Any datasets in the agency's enterprise data inventory that can be made publicly available must be listed at (Chula Vista public website) in a human- and machine-readable format that enables automatic aggregation, to the extent practicable. This public data listing should also include, to the extent permitted by law and existing terms and conditions, datasets that were produced through agency-funded grants, contracts, and cooperative agreements (excluding any data submitted primarily for the purpose of contract monitoring and administration), and, where feasible, be accompanied by standard citation information, preferably in the form of a persistent identifier.
3. Create a process to engage with customers to help facilitate and prioritize data release - Agencies must create a process to engage with customers, through their data pages and other necessary means, to solicit help in prioritizing the release of datasets and determining the most usable and appropriate formats for release. Agencies should make data available in multiple formats according to their customer needs.
4. Clarify roles and responsibilities for promoting efficient, effective data release practices - Agencies must ensure that roles and responsibilities are clearly designated for the promotion of efficient and effective data release practices across the agency, and that proper authorities have been granted to execute on related responsibilities, including:
    - Communicating the value of open data to internal stakeholders and the public;
    - Ensuring that data released to the public are open, as appropriate, and a point of contact is designated to assist open data use and to respond to complaints about adherence to open data requirements;

- Engaging entrepreneurs and innovators in the private and nonprofit sectors to encourage and facilitate the use of agency data to build applications and services;
- Working with agency components to scale best practices from bureaus and offices that excel in open data practices across the enterprise;

4. Strengthen measures to ensure that privacy and confidentiality are protected, and that data are properly secured

Agencies must incorporate privacy analyses into each stage of the information's life cycle. In particular, agencies must review the information collected or created for valid restrictions to release to determine whether it can be made publicly available, consistent with the presumption in favor of openness, and to the extent permitted by law and subject to privacy, confidentiality pledge, security, trade secret, contractual, or other valid restrictions to release. If the agency determines that information should not be made publicly available on one of these grounds, the agency must document this determination with Chula Vista Law Department.

Implementation

As agencies take steps to meet the requirements in this Policy, it is important to work strategically and prioritize those elements that can be addressed immediately, support mission-critical objectives, and result in more efficient use of taxpayer dollars.

Agencies should consider the following as they implement the requirements of this Policy:

1. Roles and Responsibilities

Agency heads must ensure that CIO is positioned with the responsibility and authority to implement the requirements of this Policy in coordination with Chula Vista's Chief Financial Officer, and Chief Information Security Officer (CISO). The CIO should also work with Chula Vista's public affairs staff, open government staff, web manager or digital strategist, program owners and other leadership, as applicable.

2. Resources

Policy implementation may require upfront investments depending on the maturity of existing information life cycle management processes at individual agencies. Agencies are encouraged to evaluate current processes and identify implementation opportunities that may result in more efficient use of taxpayer dollars. However, effective implementation should result in downstream cost savings for the enterprise through increased interoperability and accessibility of the agency's information resources. Therefore, these potential upfront investments should be considered in the context of their future benefits and be funded appropriately through the agency's capital planning and budget processes. Some of the requirements in this Policy may require additional tools and resources. Agencies should make progress commensurate with available tools and resources.

12.3.3 Data Ownership Policy

This document is provided to City of Chula Vista, CA, as a set of recommended inputs and guidance which may form the basis for a formal Policy.

The City of Chula Vista seeks to deliver efficient, effective, and improved customer services at the lowest possible cost to its residents and businesses. One way the City can identify opportunities for improved delivery of services is through the effective use of data. A strong Data Governance and Data Management Policy can help ensure that potential is maximized by providing a framework for the proper use, storage and management of data. As many agencies work together to deliver services to our customers, a key component is a clear Data Governance policy, which outlines the expectations for data access, availability, and management to ensure cross-functional decision-making, accountability, data integrity, and data availability.

This Data Governance and Data Ownership Policy defines the roles and responsibilities of Chula Vista staff, contractors, and consultants with internal and external parties in relation to data access, retrieval, storage, disposal, and backup of data assets. More generally, data policies are a collection of principles that describe the rules to control the integrity, security, quality, and usage of data during its lifecycle.

The purpose of this Data Governance and Data Ownership Policy is to:

- Define the roles and responsibilities for different data creation and usage types, cases and/or situations, and to establish clear lines of accountability;
- Develop best practices for effective data management and protection;
- Protect the City's data against internal and external threats (e.g. breach of privacy, breach of confidentiality, or security breach);
- Ensure that the City complies with applicable laws, regulations, exchange and standards;
- Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data.

Data Governance and Data Ownership Policy Action Plan

1. ***Establish Data Governance Team (DGT)***
2. ***Identify and Inventory Data Systems.*** Led by the Business Owner, each department shall review and identify its currently available data to develop an inventory of systems that store municipal data. If not already in existence, the inventory shall be completed ninety (90) days after this policy takes effect. Each department shall be responsible for updating its systems and the Business Owner shall provide updates during the regular governance meetings.
3. ***Identify Relevant Business Owners and SSDMs.*** Each department is responsible for identifying individuals to fulfill the roles of Business Owner and Source System Data Manager.
4. ***Identify Subject Matter Experts (SME) of Source System –*** Each system must have a designated SME.
5. ***Specify Operational and Security Controls for Data –*** Define and review recommended access controls; obtain approval; implement.

Data Governance and Data Management Concepts

The Dictionary of Data Management defines Data Governance as "the exercise of authority, control, and shared decision making (planning, monitoring, and enforcing) over the management of data assets." Data governance initiatives provide the foundation to develop appropriate data management protocols and procedures.

Data Management is the process that puts governance policies into action. Governance provides a framework; thereafter, you can define areas for management (such as security, database, and document control) and infrastructure or architecture management. The governance establishes the why and who for data accessibility and control, while management sets the where and how.

It should be noted that data governance and data quality are not synonymous but are closely related. *Data quality* is the measurement of data accuracy, completeness, availability, and effectiveness. Data governance policies apply guidelines to this vetted data.

What is a Data Governance Policy?

A data governance policy is a set of rules for safeguarding an organization's data assets. Data governance policies center on establishing roles and responsibilities for data that include access, disposal, storage, backup, and protection.

Data governance policies apply to everyone within the enterprise: staff, leadership, and agencies. To establish a governance structure, a team or committee should be formed to develop the goals, mission, and vision for data oversight. The team is primarily responsible for stewardship of the data; that is, the proper care of data assets. In an organization the size of Chula Vista, this stewardship role likely falls to a team, which may be named the Data Governance Team (DGT) or equivalent.

The team can be composed of information analysts, IT personnel, subject matter experts, and project managers to provide expertise; however, City management and senior agency staff can offer the balance needed for effective, proactive governance.

Data Governance Team (DGT) Responsibilities

Once a governance team is in place and sets its goals, the group can then outline a policy to structure appropriate data controls, including access, availability, and methods to ensure quality. From the initial vision and mission statements, they can develop a framework to hand off the enactment of data management. Once in place and deployed, a governance team's work and stewardship continue with a focus on monitoring, observation, and reporting. The team also handles issue resolution and analysis to support data acquisition strategies, compliance, and financial priorities to drive continuous improvement initiatives.

Goals and Benefits of Data Governance

The primary goal of governance is to assure the integrity of data assets through accountability, consistent data distribution policies, processes, and procedures, standardized systems, and education. The benefits include the following:

- Improve data quality (sometimes through standardized processes)
- Deliver trustworthy information
- Create confidence with high-quality, consistent data
- Make intelligent business decisions
- Decrease costs and improve efficiency while reducing the risk for regulatory fines
- Drive optimization and effectiveness across agencies;
- Enable better strategic planning, risk management, and compliance;
- Establish better collaborative opportunities across organizations and departments;
- Improve data security by identifying vulnerabilities and remediating;
- Increase data value;
- Resolve data problems;
- Support data-driven customer service initiatives;
- Comply with regulations;
- Improve productivity and reduce error with high quality data;
- Enable continual data improvement initiatives.

Scope

This policy applies to all data used in the administration and operation of the City and all its agencies and offices. This policy covers, but is not limited to, data in any form, including print, electronic, audio visual, video, backup and archived data.

This policy applies to all City of Chula Vista, CA staff, contractors and consultants.

Data Governance Roles and Responsibilities

This section enumerates the data governance roles and enumerates the responsibilities of each role.

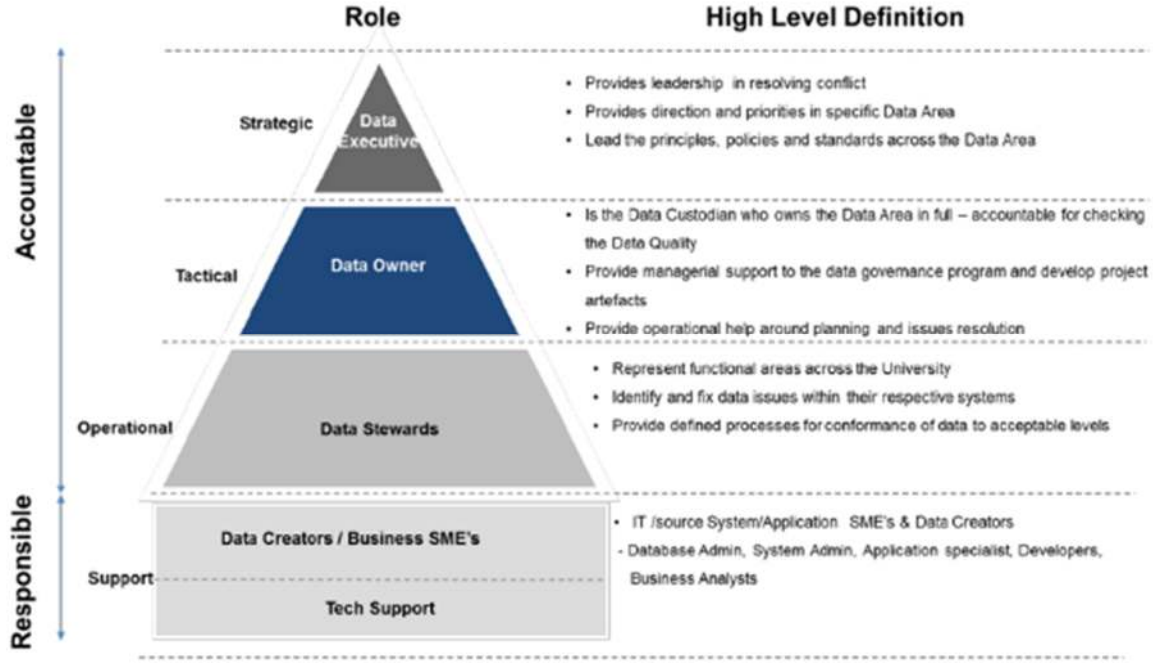


Figure 12-1 Data Governance Roles and Responsibilities

Data Governance Roles and Responsibilities

The following table outlines the responsibilities of the following Data Governance Roles.

Table 12-1 Data Governance Roles and Responsibilities

Role	Responsibilities
Data Governance Team (DGT)	Data Governance Team is responsible for the overall management of the City's data governance.
Data Executive	Data Executive supported by a Business Owner has the responsibility for the management of data assigned within their agency or scope of responsibility.
Business Owner	Business Owners are assigned by a Data Executive and are responsible for ensuring effective protocols are in place to guide the appropriate use of their data assets. Access to, and use of, institutional data will generally be administered by the appropriate Data Owner. Data Owners (or a delegated Data Steward) are also responsible for ensuring that all legal, regulatory, and policy requirements are met in relation to the specific data or information asset. Data Owners are responsible for ensuring that data conforms to legal, regulatory, exchange, and operational standards.
Source System Data Manager	Every data area must have one or more Source System Data Manager, who are responsible for the quality and integrity, implementation and enforcement of data management within their agency. The Data Steward will classify and approve the access, under delegation from a Data Owner, based upon the appropriateness of the User's role and the intended use. Where necessary, approval from the Data Executive/Data Owner may be required prior to authorization of access.
Data Creators	Data Creators may be systems that create data (e.g. – transaction systems or billing systems), or capture data (e.g. – web applications, smart applications, etc.).
Business Subject Matter Experts (SME)	Business SMEs are business and technical subject matter experts in relation to the data or information asset.
Data Users	Data Users are consumers of the data. These data users may be Chula Vista employees, contractors or staff. They may also be external users in the Open Data model.

Considerations on Data Management

Data Quality and Integrity

- Data Creators and Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access

- Data records must be kept current throughout every stage of the City's business and operations workflow, in an auditable and traceable manner. Data should only be collected for legitimate uses and to add value to the City and its residents. Extraction, manipulation and reporting of data must be done for valid business or analysis purposes.
- As appropriate, before any data (other than publicly available data) is used or shared outside the City, verification with the Data Steward is required to ensure the quality, integrity and security of data will not be compromised.

Classification and Security:

- Appropriate data security measures must be applied at all times to assure the safety, quality and integrity of City data.
- Personal use of institutional data, individual data, or public safety data, including derived data, in any format and at any location, is prohibited.
- Records stored in an electronic format must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorized user(s) Similarly, data in the City's data repositories and databases must also be stored in a manner that will restrict access only to authorized user(s).
- This Policy applies to records in all formats (paper, digital, audio-visual or video) whether registered files, electronic documents, emails, online transactions, data held in databases or on tape or disks, maps, plans, photographs, sound and video recordings, or any other storage and retrieval medium.

Other Considerations on Data Management

Open Availability of Data. The City is a steward of the data that it collects from residents and visitors. No one person, department, division, or group has exclusive access to City of Chula Vista data. While departments are responsible for the management of data they have collected, any other department can request access to any data. These requests may be subject to legal limitations to protect personally identifying information (PII), such as HIPAA and CJIS, as well as any internal security procedures and guidelines the City of Chula Vista has developed to protect data. If a request for data is denied, the reasons for denial shall be provided to the requesting agency, which will have an opportunity to modify its request.

Data Collection. Data will be collected in a lawful and appropriate manner in accordance with the requirements of applicable legislation and any additional processes agreed upon by the departments requesting and providing the data in order to protect PII or sensitive data.

Automatic Extraction of Data. If data is shared among or between agencies, for example to improve the delivery of a service or so City Manager can monitor the performance of an agency, that data shall automatically be extracted, transferred, and loaded to a secure, external computer warehouse. The location of the data must be approved by DGT to ensure there are no unnecessary restrictions preventing access to the data. Automatic extraction and collection will allow departments to efficiently and immediately use data. If a department has concerns regarding security or personally identifying information (PII), it will document those

concerns and develop a separate agreement with the requesting department outlining why the information is not being automatically extracted, the schedule for extraction, and the safeguards established for data of concern. All efforts will be made to ensure that data is not pulled during high volume times to minimize disruptions of departmental operations. Evaluations of current data sharing processes will be evaluated at the regular meetings between the Chief Data Officer, the Business Owners, and the Source System Data Managers.

Data Use & ***Disclosure.*** Data will be used and disclosed in a lawful and appropriate manner in accordance with the requirements of applicable legislation and any signed City of Chula Vista data use agreement. Unless it is specifically requested through a public records request, data will not be redistributed in its raw form without the specific written permission of the originally collecting department. But aggregated data that does not contain personally identifiable information (PII) may be shared as part of reports to the city and outreach to the general public. When aggregating data, departments specifically review outliers to minimize the extent to which those outliers allow for personal identification.

Data Retention and Disposal Data will be retained and disposed of in a lawful and appropriate manner in accordance to the City of Chula Vista 's Security and Record Retention policies. If a department has extracted data from another department, it is responsible for disposing of that data at the end of the appropriate retention period or, if it chooses to retain the data for a longer period of time, informing the original collecting department of its choice and appropriately publicizing that information in compliance with California law.

Responses to Records Requests. Each department is responsible for responding to records requests. For the purposes of California public records laws, the originally collecting department shall be considered the department that "owns" the data. Extracting departments shall be responsible for responding to a request only if the requested record were retained by the extracting department and not by the original collecting department beyond the relevant retention period.

Third Party IT Solutions & ***IT Procurement.*** A department which believes it does not have the technology necessary to achieve one of its goals must approach IT Governance to determine whether there is an in-house solution before contacting any outside vendors. If an in-house solution is not available, the Purchasing Division, in conjunction with the Enterprise Technology Solutions department and the IT Governance team, must work with the department and the third-party vendor to ensure there is specific language included in the contract to ensure data will remain properly open to the City of Chula Vista for access and analysis. IT Governance, the Chief Data Officer, and the Department should also consider:

- Accessibility – Access to system is managed and appropriately limited, and whether the contract involves use of products from other vendors for whom access must also be limited.

- Control – Who owns the data; whether the provider may change the agreement at its sole discretion or with approval; scope of any licenses.
- Services – Which services are provided; service levels to problem or enhancement requests; functionalities; whether purchased product or service interface with current or planned technology at Chula Vista; how long features will be supported; how frequently maintenance will be performed and with what notice.
- Security – Whether vendor security standards conform to Chula Vista security standards.

12.3.4 Smart Cities Readiness Policy

Introduction

As technology plays an increasingly large role in the way we live, cities have begun to realize the benefits of putting it to use in improving sustainability, workability, and livability. While a city may be "smart" in many ways, a Smart City or Smart Region is essentially a place where residents, industries, and government agencies are able to realize a clear, shared purpose through better decisions and more effective actions. This is not necessarily defined by the number or kind of devices and technologies in use; rather, it is a vision, shared by many, in which innovation and connectedness lead to increased well-being for all.

Smart Cities are enabled generally by the Internet of Things (IoT). The IoT is being driven by the increased sophistication and reduced costs associated with wireless, Bluetooth and sensor technologies, coupled with the advent of cloud computing, which places storage and computing power in the cloud. All devices around us are undergoing technological re-imagination to incorporate technology to make them "smart." Increasingly simpler and cheaper devices can be employed by cities to connect municipal assets and functions that generate more and more data – enabling more efficient and effective management of services and programs.

What it means to be a Smart City varies across communities. In some cases, the term refers to a high level of usage of the IoT in which robots, autonomous transportation, and drones are used throughout a community, creating a more cost-effective way to manage traffic, control energy consumption, and increase convenience. In other cases, it may to an ecosystem of innovation in which quality of life is improved by facilitating communication between citizens and governments, encouraging entrepreneurship and creativity, and creating more desirable areas to live, work, and play.

Scope

Advancing technologies place cities at the center of innovation: autonomous vehicles revising the concept of traffic and traffic signals; Wi-Fi transforming the way information is used and accessed; facial recognition technology transforming building security; shared vehicles allowing a move away from parking costs, land use, and emissions; integration of renewable energy sources and smart metering technology for water, electric and gas; smart street lighting poles providing vertical assets for wireless data via 4G/5G and Wi-Fi; wireless data, smart lighting and embedded sensors powering numerous applications to allow for faster responses for public safety; and integration of systems with customer feedback loops to enhance and improve customer service for residents and visitors. These initiatives include broadband services, collaboration

opportunities, public safety applications, and future energy and utility management functions and features as shown below.

Smart City initiatives require high bandwidth network connectivity for transmission of large and growing amounts of data. Generally, cities can obtain this fiber-optic cable-based high bandwidth connectivity in either of two ways. Traditionally, area service providers sell high bandwidth (broadband) to cities as a service on their own infrastructure. The service is priced as a retail service from relatively few providers and many cities are finding it to be unaffordable in both the short and long run. The alternative is to use and expand city assets in public rights-of-way, on a planned and strategic basis, as proposed here, to provide Smart City connectivity. Municipal broadband networks provide affordable means for implementing Smart City initiatives for health, education, public safety, mobility, livability and economic growth. Therefore, as communities invest in fiber infrastructure, they are constructing foundational communications networking useful to support a multitude of technology-based initiatives that require connectivity.

It is important to note that broadband networks are not all that is required for Smart Cities. Organizational and human factors must be provided for to foster the necessary collaborations and investment in human capital. Ultimately Smart Cities initiatives are layered, involving network facilities infrastructure, with connected devices (cameras, sensors, Wi-Fi, etc.), and the data from these devices which allows capabilities to be embedded in daily practices based on collaboration among organizations and departments. Implementation of Smart City applications originates the proverbial "fire hose" of data – the collection and use of which must be planned for and managed. A concrete plan to manage the data generated by the Smart City is essential and should be developed during evaluation of Smart City applications, and before their implementation. Smart City data streams are too large to manage and use without processing the data.

The table below lists some of the many smart city applications and devices that can increase efficiency, sustainability, and usability in delivering key services to the community.

Table 12-2 Smart City Technologies

Transportation Congestion Sensors	Lighting
Water and Wastewater Monitoring	Fire Detection
Parking Apps and Kiosks to Coordinate with Smart Meters	Self-Driving Cars, Shuttling People In and Out of the City of Making Deliveries
Bridge Inspection Systems	Solar Panels
Energy Monitoring	Smart Logistics/Freight
Waste Management Sensors	Vehicle Fleet Communications
Drones for Public Safety and Infrastructure	Monitoring Cameras
Body Cameras	Wearable Detection

Policy Requirements

A vast and growing body of studies, information, products and implementations that cover the Smart City exists. One of these is the report produced by The National League of Cities (NLC) on trends in Smart City development.[26] Smart City applications require three things working together for effectiveness: computing and telecommunications infrastructure to collect data, software applications and tools to analyze and interpret the data, and a collaborative environment in the organizations that innovate, create and use Smart City applications.

National League of Cities' Smart City recommendations are:

1. ***Cities should consider the outcomes they want to achieve*.** "Data collection is not an end in itself." Initiatives need to be clearly defined. Consider what the need is, not just what other cities are doing.
2. ***Cities should look for ways to partner with universities, non-profits and the private sector*.** Cities can even partner with other cities. There are many benefits to partnering and collaboration, including access to experience, shared risks of development, and providing project continuity. Downsides to collaboration also need to be considered in structuring any partnership.
3. ***Cities should continue to look for Smart City best practices*.** Technologies are new and at present there is significant variability and a lack of agreed standards. The National Institute of Standards and Technology is working on this matter.

The Smart Cities Council published a "Smart Cities Readiness Guide"[27] containing detailed information on Smart City drivers and barriers, benefits, "beyond silos," and City responsibilities. City responsibilities and opportunities are outlined as follows:

- ***Built Environment***: Leading and planning for "smart buildings" powered by ICT, using sensors, meters, systems and software to monitor and control a wide range of building functions including lighting, energy, water, HVAC, communications, video monitoring, intrusion detection, elevator monitoring, and fire safety.
- ***Digital City Services***: Switching to digital delivery of city services to increase citizen engagement, employee productivity, competitiveness, citizen satisfaction, and simultaneously, to reduce cost. Services are delivered via the web, smartphones and kiosks, which can require implementation of new technologies, and attitudes or approaches.
- ***Energy***: Smart energy is a priority for Smart Cities, which start with smart energy systems.

[26] *NLC Smart Cities Report.*
[27] http://rg.smartcitiescouncil.com/readiness-guide/article/drivers-whats-driving-smart-cities

- ***Health and Human Services***: Smart Cities ride the transformation wave provided by advances in ICT to transform the delivery of essential health and education services since "an educated and healthy city is a wealthy and successful city."
- ***Ideas to Action***: A "roadmap" linked to a City's vision document and comprehensive plan is necessary to turn ideas to action, and make technology serve the City's larger goals. The path to a Smart City is not quick, and targets are needed for clear goals to motivate citizens and permit any required course corrections.
- ***Mobility and Logistics***: Population growth and congestion make this a critical area for the Smart City. Traffic congestion is wasteful and costly to the economy – both directly and indirectly. There are a variety of action steps and targets that can provide for safer, more efficient transportation, including accommodating electric and autonomous vehicles and smart parking, among others.
- ***Public Safety***: Public safety relies on a lengthy list of infrastructure, agencies and people to keep the public safe. ICT in the Smart City fosters quicker and smarter responses without wasteful duplicated effort to save lives, property and resources.
- ***Smart Payments and Finance***: Digitalizing both disbursements and collections generates significant savings and increases operational efficiency.
- ***Smart People***: A new city hall mindset that is more open, transparent and inclusive to build two-way communications and create stronger initiatives.
- ***Telecommunications***: An adequate telecommunications infrastructure is vital for business and community development and underlies the Smart City.
- ***Waste Management***: Population growth and accelerating consumption have created a rising tide of waste, outpacing the rate of urbanization. Smart cities can collect and process waste more efficiently and recover materials which have value, with a beneficial impact on public health, the environment and sustainability/zero waste, and cost control.
- ***Water and Wastewater***: Like energy, water is critical to everyday life. There is also an energy–water nexus, meaning it takes water to produce electricity, and electricity to pump water. The Smart City provides intelligence for both energy and water systems and enhances the platform for economical and sustainable production of both energy and water.

12.3.5 Dig Once Policy

"Dig Once" refers to policies and/or practices that foster cooperation among entities (especially utilities) that occupy public rights-of-way, to minimize the number and scale of excavations when installing infrastructure (especially telecommunications[28]) in public rights-of-way. Dig Once has

[28] Occupants of the public rights-of-way include gas, water/sewer and electric public utilities and several telecommunications providers that seek permission to encroach on public rights-of-way, including cable TV companies, competitive telecommunications companies, and wireless communications companies.

numerous substantial benefits, including promoting and supporting the placement of broadband infrastructure (e.g., fiber-optic cable and conduit); reducing the consequences and disruptions of repeated excavations (traffic disruption, road deterioration, service outages, and wasted resources), and enhancing service reliability and aesthetics. Dig Once accomplishes the goal of minimizing costs of constructing separate trenches and facilities via shared costs of construction. Sixty to eighty percent of a fiber optic network's capital costs are from opening and closing the ground for facilities placement (e.g., trenching, boring, placing conduit). The cost savings from shared construction therefore are significant. The Federal Highway Administration estimates it is ten times more expensive to dig up and then repair an existing road to lay fiber, than to dig support structure for fiber (e.g., conduit) when the road is being fixed or built. [29] According to an analysis by the Government Accountability Office, Dig Once policies can save from 25-33% in construction costs in urban areas and approximately 16% in rural areas. In addition, development of Dig Once standards and guidelines for deployment of conduit and fiber will facilitate economic development and growth, as it enables cost-effective staged or gradual deployment of broadband infrastructure.

Dig Once policy discussions generally address the planning and coordination process for construction projects in the public rights-of-way. But the concept can also extend to required placement of conduit for fiber optics whenever the ground is opened, as expressed in recent Congressional legislation. This concept was embodied in the Broadband Conduit Deployment Act of 2018, which required the inclusion of broadband conduit during construction of any road receiving federal funding.[30] Similarly, the State of California has passed legislation (AB 1549) which requires the Department of Transportation to develop guidelines to facilitate installation of broadband conduit on state highway rights-of-way.

The Dig Once concept has recurred in Chula Vista in connection with discussions with developers and revising developer agreements as well as transportation planning. The City of Chula Vista has therefore expressed interest in exploring and adopting Dig Once policies.

Policy approaches can differ between detailing specific Dig Once processes in ordinances (e.g., San Francisco) or stating the policy direction to require coordination of projects in the roads and rights-of-way, leaving specific implementation and management to designated city officials (e.g., Director of Public Works) on a less formal basis than specific ordinance requirements.[36] The latter approach may work best for Chula Vista, given that several departments have responsibilities in or regarding the public rights-of-way. Magellan Advisors recommends that the City take this approach to coordinate of projects in the rights-of-way to promote

---

[29] https://eshoo.house.gov/issues/telecommunications/eshoo-and-mckinley-introduce-dig-once-legislation-to-reduce-cost-of-expanding-broadband/

[30] *Id.*

expansion of broadband infrastructure, reducing disruptive repeated excavations which cause traffic disruption, road deterioration, service disruptions and wasted resources.

A draft Dig Once policy is attached as Appendix A.

Chula Vista's Developer's Agreements could be updated. Dig Once / Joint Trench policies could be developed and finalized. Additional requirements to be considered include:

- Requirement to coordinate installation, construction and maintenance work in the rights-of-way with the City, and with other utilities;
    - Requirement of all occupants of the rights-of-way to submit plans quarterly for major excavation work in the next [12 months] to the City Engineer, in an acceptable format;
        - Recognize it is an estimate and plans do change;
        - Provide for protection of confidential business information;
    - The plans of all occupants of the rights-of-way are reviewed by the City Engineer to identify conflicts and opportunities for coordination of activities.
- Notification of all providers of the opportunity to join the open trench and to coordinate efforts for multiple parties to join the dig;
- Provision for installation of public utility infrastructure (e.g., conduit, tube, duct or other structure for enclosing telecommunications fibers, wires, cables) in each excavation exceeding a set distance (e.g., 300 linear feet) (with exemption for good reason granted by the City Engineer);
- Provision of specified conduit space for the City for its use; and,
- Imposition of a moratorium on excavations affecting City roads for five years following new pavement.

Furthermore, the City could consider requiring any licensee who is permitted to install facilities underground to provide duct/conduit space for the City's use to extend its network. The City could use the following language in policy or ordinance to express that requirement:

When a Grantee is installing communication infrastructure in City property licensed under this Title, the City, in the sole discretion of the Directors, may require said Grantee to also install conduit, inner duct, and fiber-optic cable ("underground communications infrastructure") on behalf of the City. A Grantee is required to obtain confirmation in writing from the City about whether the City requires the installation of underground communications infrastructure for areas located within the Grantee's proposed construction plan.

1. *In addition, to the installation of underground communications infrastructure, the Grantee may be required, in the sole discretion of the Directors, to install such vaults, manholes,*

hand-holes, and other appurtenances and facilities as are necessary or needed to accommodate installation and connection of underground communications infrastructure.

2. *All construction and installation required in this Section shall be accomplished by the construction standards set forth in this Chapter.*
3. *All underground communications infrastructure installed by Grantees shall be conveyed and dedicated to the City either with or as part of the dedication of the public street and/or rights-of-way to the City.*
4. *The City will bear a pro rata share of the materials costs associated solely with underground communications infrastructure that is installed for the City's use and management.*
5. *All Grantees shall be required to use available dark fiber (currently unused fiber-optic strands) within then existing infrastructure or to locate their cable, wire, or lines within such available existing conduit unless it can be demonstrated to the reasonable satisfaction of the Directors that such use or location is not technologically feasible or reasonably practicable. Fiber-optic cable and strands as well as conduit shall be allocated to the Grantees on a first-come, first-served basis; provided, that the City may reserve capacity within such fiber and conduits for its own use; and provided further, that the Directors may reasonably adopt additional rules for fiber-optic cable or strand and conduit allocation in order to ensure that all Grantees have reasonable access to the City's rights-of-ways and that no barrier to entry or competition result from the allocation of cable, strand, or conduit space.*
6. *The City reserves the right to charge reasonable fees for the use of fiber-optic cable and fiber-optic network conduit and attendant accessories, facilities, and infrastructure installed pursuant to this Section, to the extent consistent with and as limited by federal and state laws and resolutions.*

13. Wireless Systems Security

13.1 BACKGROUND AND GENERAL REQUIREMENTS

Municipal governments must meet rising needs for city services on ever tightening budgets. For many cities with a reduced tax base and federal or state subsidies, the challenge is to maintain or improve basic services and public safety with fewer personnel. As in any enterprise, efficient access to data, network resources and the Internet is a necessity, not an option, for improving productivity with fewer resources. One significant difference between municipal governments and many enterprises, however, is that many City services are performed outdoors. Tasks such as the following are performed outside of a City government building, where access to a reliable network is not a given:

- Building and fire code inspections
- City parks and recreational facility upkeep
- Code enforcement
- City maintenance
- Traffic monitoring, community policing, and other public safety duties

Delivering reliable, high-speed network access outdoors is much more problematic than providing this kind of access inside a building. Adding to the challenge is the desire of many local governments to go beyond baseline services and do more for their citizens and community. Initiatives to stimulate economic development, making technology accessible to more constituents, or encourage tourism are widespread, based on the principle that a vibrant local economy and residential base will improve the financial health of the City.

One common theme of these initiatives is affordable broadband access—in downtown areas where economic revitalization is the goal, in residential neighborhoods where the current broadband offering may not be within the means of lower-income families, and in business districts that want to attract conferences, business travelers, and tourists. But delivering this access is another matter. Incumbent service providers may not provide affordable access to all areas. In some cases, broadband access may not be available at all, especially in lower-income or less populated areas.

Delivering network connectivity to mobile public safety and City personnel raises a whole new set of challenges. With no fixed location, users face two choices: either return to an office to gain network access or use wireless cellular wide area networks (WANs). Having to return to the office is not efficient—the time and travel required from the field to a building for network connectivity result in undue delays. The effectiveness of WANs depends upon the application and data needs. WAN download and upload speeds are typically much slower than LAN speeds. For tasks that require large files, pictures, and video, using a WAN connection may be more frustrating than returning to an office.

13.2 PROPOSED SOLUTION FRAMEWORK

An alternative method of providing cellular communication services is to deploy high-speed wireless networks based on the IEEE 802.11 standards, also known as wireless LANs (WLANs) or Wi-Fi. When multiple access points are used to cover outdoor areas, they are commonly referred to as wireless mesh networks. However, deployment of a wireless mesh network may raise questions about the ability to extend the City's network outdoors and keep it secure. While the wireless medium has specific unique characteristics, IT managers can take comfort in the fact that essential WLAN security measures are not very different from those required to build strong wired network security. Thus, by employing the proper WLAN security measures, IT administrators can maintain corporate privacy. This paper discusses different users, applications, and deployment models for wireless technology for outdoor wireless network deployments

13.2.1 Outdoor Wireless Network Applications and User Types

Understanding the different users and the anticipated applications for a wireless network is an important first step in any discussion of security measures. As with an indoor enterprise network, different types of users and applications necessitate different security measures. In general, there are three basic usage models for outdoor wireless networks:

- Municipality and city agency applications
- Public safety applications
- Public use applications, including use by residents, businesses, and tourists

Municipality and City Employee Applications

For many cities, streamlining workflow in the field represents an enormous potential reduction in manpower and increase in productivity. A primary goal is enabling employees to remain in the field instead of having to return to a central office to receive the next job or modify their route as a result of changing conditions. Using wirelessly enabled PDAs or laptops allows city personnel to receive job assignments, plans, or research material or equipment databases while in the field. Bar-code scanners can be used for asset or service tracking and can provide instant updates to other team members. With wireless mobility, city personnel can become more responsive to ad-hoc assignment changes.

Another important application is automatic meter reading, which is currently a time-intensive task. A wireless network can aggregate data from automatic meter reading (AMR) solutions in areas of a city where a fiber network may not be available. This eliminates the need for manual reading, which is not only expensive, but may also be a safety risk for meter reading personnel. Even if meter reading is currently accomplished wirelessly by personnel in the field, significant time and money can be saved by eliminating this step. Another use of AMR is the real-time monitoring of water and electricity usage data, creating more visibility into consumption. With real-time monitoring, agencies can determine if a high usage of electricity or water at any given time could

be a result of faults in the system, such as water leakage from broken pipes. A quick response can improve customer satisfaction with the agencies' performance in emergency situations.

Public Safety Applications

Public safety applications cover a broad spectrum of potential users: police, fire, emergency medical services, 911 centers, airports, and transit agencies. These users need levels of system coverage, capacity, security, and control that commercial carrier systems often cannot achieve. What's more, public safety agencies are often accustomed to deploying and managing their own private systems. Some examples of applications that improve the effectiveness of public safety agencies include the following:

- Mobile data access—Immediate full-text access to DMV records, warrants, mug shots, criminal records, and Amber Alerts (high-priority bulletins about missing children) to speed decision making and increase safety.
- Streaming video and digital images—Video surveillance from government buildings and businesses to gauge the nature of the response needed.
- Building schematics and plans—Immediate access to schematics and plans as critical aid to fire safety personnel in search and rescue operations.
- Ad-hoc wireless networks—Critical for facilitating local communication among emergency responders.

Mobile devices, such as laptops, tablets, personal digital assistants (PDAs) and smart phones, are most commonly used for these applications. The devices are generally used in response vehicles, or "ruggedized" for use outside the vehicle. Because of the highly sensitive nature of much of the information, security measures for these applications must be much more stringent than for municipal or public usage applications.

Public Use Applications

Public use applications represent the most widely discussed area of outdoor wireless networks based on Wi-Fi. The permutations range from free, pervasive outdoor deployment in city centers for use by anyone to daily fee-based systems to monthly subscriptions for businesses and residents in select areas. Applications using the network therefore will be broad, but in general, the primary goal is to provide a high-speed broadband connection with the security of that connection left up to the user. While the laptop is currently the primary device for connecting to the network, a wide range of devices that are designed to connect to public Wi-Fi networks are becoming available. Examples include mobile data devices such as the RIM Blackberry, phones that operate as Wi-Fi and even cameras that are enabled with embedded wireless LAN clients.

Multi-Use Networks Are Becoming Standard

An initial network deployment may begin with a single user and application type to prove out the design but will likely quickly migrate to a multiuse scenario. Even if this is not specifically planned

for, the impact Wi-Fi has on outdoors is much the same as indoors. Once awareness of an outdoor WLAN exists, there is an almost immediate desire by multiple constituencies to use it. The implication for those planning and designing the network is enormous: the infrastructure must be able to support multiple users with varying endpoint devices that will likely require different authentication and security methods.

Outdoor Wireless Deployment Architectures

A few highly publicized plans to cover entire cities with Wi-Fi have received significant attention; however, multiple deployment models exist. Outdoor wireless LAN deployments fall into one of three distinct categories: hotspots, hot zones, or a pervasive wireless deployment. Each type of deployment has distinct requirements that require sufficient hardware and personnel to implement and support.

Hotspots

Hotspots are characterized by a deployment of a single access point. The term is commonly used to refer to a single wireless LAN access point within a café or restaurant, but it is also applicable when that access point is deployed outdoors. In fact, many cities find the simplest entry point into an outdoor wireless network is to create hotspots of coverage outdoors around government buildings—fire stations, police stations, courthouses, field service depots, and so on—allowing city personnel to gain high-speed connectivity at various locations around town without having to return to headquarters.

Hot Zones and Pervasive Wireless Deployments

Deploying multiple access points to create a single contiguous coverage area creates a hot zone. Hot zones typically concentrate a wider coverage in dense areas with a higher capacity to support many users. Downtown business districts, city government campuses, recreational parks and venues, and harbors or marinas are all common locations for WLAN hot zones. Pervasive wireless deployments are simply extensions of hot zones across an entire municipality or a significant portion of it. Aside from the obvious increase in access points needed with a larger deployment, the main difference between a hot zone deployment and a pervasive wireless deployment is the requirement for more backhaul points of broadband connectivity to the edge access points, allowing data traffic to move more quickly to the Internet and reducing congestion at the access level.

Because hot zones and pervasive wireless deployments consist of multiple access points, these deployments must support two requirements:

- Uninterrupted roaming of mobile devices across multiple subnets
- Easy backhaul connectivity for the access points

Uninterrupted Roaming of Mobile Devices Across Multiple Subnets

Larger outdoor wireless deployments are likely to place access points across subnet boundaries. Similar to an indoor wireless LAN deployment, outdoor wireless deployments require the infrastructure to support uninterrupted connectivity as a mobile device roams across a subnet boundary. The software client allows applications to stay active when a user travels between wireless (Wi-Fi or cellular) coverage areas. Police, fire, and emergency responders requiring real-time data or video feeds and transportation system telemetry are all examples of situations in which devices need to maintain mobile connectivity across large geographic distances.

Easy Backhaul Connectivity

There are multiple reasons for limiting the requirement for backhaul to each access point when deploying a hot zone or pervasive Wi-Fi network. Wireless access points typically have a range of 1000 to 2000 feet outdoors, depending on the density of buildings, foliage, and other obstacles; as a result, they must be placed fairly close together to create pervasive coverage. A good average estimate for many suburban cities is 20 to 25 access points per square mile. The higher the access point is placed, the better its range will be. Desirable mounting sites include utility poles, water towers, and the top of city buildings. Existing backhaul at these types of sites is highly unlikely. And the cost of providing network connectivity to these sites is much higher than pulling cable inside a building. To address this problem, linking access points over the wireless medium, also known as mesh networking, allows significant reduction in the number of backhaul points, dramatically reducing the cost of a hot zone or pervasive wireless network.

Other Security Considerations

Layer 2 and layer 3 encryption methods are considered by many experts as not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the application layer, using technologies like secure socket layers (SSL), secure shell (SSL), Pretty Good Privacy (PGP), and similar encryption technologies.

The disadvantage with the end-to-end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on", and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

The most prized resource is often access to the Internet. An office LAN owner seeking to restrict such access will face the nontrivial enforcement task of having each user authenticate themselves for the router.

Perhaps the most rigorous security to implement into WLAN's today is the 802.11i RSN-standard. This full-fledged 802.11i standard, however, does require the newest hardware), thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP (an early version of 802.11i) or the newer and better AES-CCMP-equipment. One should make sure one needs WRAP or CCMP-equipment, as the two hardware standards are not compatible.

Wi-Fi 5 and Wi-Fi 6

The next generation of Wi-Fi, known as Wi-Fi 6, isn't just a simple speed boost. Its impact will be more nuanced, and we're likely to see its benefits more and more over time. This is less of a one-time speed increase and more of a future-facing upgrade designed to make sure our speeds don't grind to a halt a few years down the road.

Wi-Fi 6 is the next generation of Wi-Fi. It'll still do the same basic thing — connect to the internet — just with a bunch of additional technologies to make that happen more efficiently, speeding up connections in the process. Current speeds are 9.6 Gbps which is up from 3.5 Gbps on Wi-Fi 5. But the fact that Wi-Fi 6 has a much higher theoretical speed limit than its predecessor is still important. That 9.6 Gbps doesn't have to go to a single computer. It can be split up across a whole network of devices. That means more potential speed for each device. Until recently, Wi-Fi generations were referred to by an arcane naming scheme that required you to understand whether 802.11n was faster than 802.11ac, and whether 802.11ac was faster than 802.11af, and whether any of those names were just made up nonsense. (Answer: sort of.) To fix that, the Wi-Fi Alliance decided to rename Wi-Fi generations with simple version numbers. So, the current generation of Wi-Fi, 802.11ac, turned into Wi-Fi 5. This new generation, previously called 802.11ax, is now Wi-Fi 6. You probably won't hear the Wi-Fi 5 name used very much since it's been around for five years and just got that name in October 2018. For Wi-Fi 6, you might see the 802.11ax name here and there, but companies largely seem to be on board with using the simplified naming scheme. Instead of boosting the speed for individual devices, Wi-Fi 6 is all about improving the network when a bunch of devices are connected. That's an important goal, and it arrives at an important time: when Wi-Fi 5 came out, the average US household had about five Wi-Fi devices in it. Now, homes have nine Wi-Fi devices on average, and various firms have predicted we'll hit 50 on average within several years. Those added devices take a toll on your network. Your router can only communicate with so many devices at once, so the more gadgets demanding Wi-Fi, the more the network overall is going to slow down.

Wi-Fi 6 introduces some new technologies to help mitigate the issues that come with putting dozens of Wi-Fi devices on a single network. It lets routers communicate with more devices at once, lets routers send data to multiple devices in the same broadcast, and lets Wi-Fi devices schedule check-ins with the router. Together, those features should keep connections strong even as more and more devices start demanding data. The story starts to change as more and more devices get added onto your network. Where current routers might start to get overwhelmed by

requests from a multitude of devices, Wi-Fi 6 routers are designed to more effectively keep all those devices up to date with the data they need.

Wi-Fi generations rely on new hardware, not just software updates, so you'll need to buy new phones, laptops, and so on to get the new version of Wi-Fi. New devices will start coming with Wi-Fi 6 by default. As you replace your phone, laptop, and game consoles over the next five years, you'll bring home new ones that include the latest version of Wi-Fi.

There are two key technologies speeding up Wi-Fi 6 connections: MU-MIMO and OFDMA. MU-MIMO, which stands for "multi-user, multiple input, multiple output," is already in use in modern routers and devices, but Wi-Fi 6 upgrades it. The technology allows a router to communicate with multiple devices at the same time, rather than broadcasting to one device, and then the next, and the next. Right now, MU-MIMO allows routers to communicate with four devices at a time. Wi-Fi 6 will allow devices to communicate with up to eight. The other new technology, OFDMA, which stands for "orthogonal frequency division multiple access," allows one transmission to deliver data to multiple devices at once. In practice, this is all used to get more out of every transmission that carries a Wi-Fi signal from a router to your device.

Wi-Fi 6 can also improve battery life. Another new technology in Wi-Fi 6 allows devices to plan out communications with a router, reducing the amount of time they need to keep their antennas powered on to transmit and search for signals. That means less drain on batteries and improved battery life in turn. This is all possible because of a feature called Target Wake Time, which lets routers schedule check-in times with devices. This feature is meant more for smaller, already low-power Wi-Fi devices that just need to update their status every now and then. (Think small sensors placed around a home to monitor things like leaks or smart home devices that sit unused most of the day.)

Wi-Fi 6 also means better security. Last year, Wi-Fi started getting its biggest security update in a decade, with a new security protocol called WPA3. WPA3 makes it harder for hackers to crack passwords by constantly guessing them, and it makes some data less useful even if hackers manage to obtain it. Current devices and routers can support WPA3, but it's optional. For a Wi-Fi 6 device to receive certification from the Wi-Fi Alliance, WPA3 is required, so most Wi-Fi 6 devices are likely to include the stronger security once the certification program launches.

13.3 CONCLUSION

Outdoor wireless networks based on IEEE 802.11 can provide a simple, low-cost method for cities and public safety agencies to improve productivity and operate more efficiently, while staying within budget. A variety of applications and users can securely and simultaneously exist on the network, ensuring the fastest possible return on investment. The wireless network delivers a unified, consistent set of network features that allow customers to bring wireless to their existing wired solutions and to extend intelligent network features and capabilities to mobile users across the City.

14. Governance

In this section, Magellan Advisors recommends two primary governance and oversight programs to provide better strategic guidance and to improve project execution through more standardized project management processes.

14.1 DEVELOP GOVERNANCE PROGRAM FOR IT OVERSIGHT

Chula Vista should formalize an Information Technology Governance Program (IT Oversight) to provide governance and management guidance to the City's telecommunications and network plans, helping to enable Smart City initiatives within City government. This IT Oversight would be focused on continuing to meet the needs and demands of City operations, prioritizing strategic initiatives for Information and Technology Services (ITS), bringing value to Chula Vista government operations while providing enabling infrastructure enhancements to support Smart Cities initiatives.

Chula Vista should plan and execute the following tasks, at a minimum:

- Create an IT Oversight Committee, charged with providing executive level input on priorities, spending allocations, and strategic initiatives. Membership in the Committee should include, at a minimum, these individuals or their designees: Director of Information and Technology Services (ITS); Director of Public Works; Director of Finance; Director of Economic Development; Traffic Engineer; City Manager's representative; and any others City chooses to include.
- Create and ratify a Charter for the IT Oversight Committee, along with defined roles, responsibilities and procedures.
- Develop infrastructure for collecting requests for strategic projects, which include initiative descriptions; identified sponsors; high-level objective statements; rough estimates of capital costs (for implementation) and operating costs (for ongoing support); and preliminary identification of possible affected departments.
- Develop a scoring metric to evaluate all proposed strategic initiatives.
- Schedule semi-annual meetings, with outputs aligned with operating and capital budget cycles, for initiative prioritization (quarterly meetings might be too frequent).
- Develop a formal plan and schedule for executing all these tasks.

14.2 DEVELOP PROJECT MANAGEMENT GUIDELINES

Chula Vista should consider establishing a basic Project Management Office (PMO) to define standard processes for high-priority projects. These standard processes could be based upon, or derived from, the Project Management Institute's (PMI's) Project Management Book of Knowledge (PMBOK). The foundation for project execution should be the implementation of project charters, scope and deliverable statements, framework for requirements, well-defined testing methodologies, and well-defined signoff on acceptance.

These project management guidance initiatives can be informed by awareness of Agile and Scrum techniques and need not be burdensome.

14.3 POLICY DEVELOPMENT

Chula Vista already has defined processes for reviewing proposed policies and for collecting input from affected internal departments and members of City management. These policies are reviewed by department heads, by City Attorney's Office, and by members of City Manager's Office. Preparation of Staff Reports and presentation to City Council for review and approval.

Magellan recommends that this policy development process be documented and formalized.

15. Valuation of City Assets

In valuing city assets to support smart city activities, the City of Chula Vista should consider the Federal Communications Commission's (FCC's) Small Cell Wireless Order, the "Declaratory Ruling and Third Report and Order" ("Order"), FCC 18-133. This order was adopted by the FCC on Sep 26, 2018 and went into effect in January 2019. The ruling is now pending review and appeal in the Ninth Circuit Court.

The Order provided guidance to municipalities and other entities in three areas related to 5G communications, especially small cell attachments. First, the Order mandated accelerated shot clock review processes for wireless carrier applications. For existing poles and other attachment bases, the shot clock was reduced to 60 days for city review and approval; for new poles, the shot clock deadline is 90 days. The report details the bases on which a municipality may challenge a permit application but imposes specific turnarounds within the shot clock window. There are no extensions for large batch applications of pole attachment.

Second, the Order provided guidance on the sizes of attachments to poles, which cannot exceed 28 cubic feet in volume. In addition, it provided flexibility to a municipality defining and publishing aesthetic guidelines for poles and attachments. Those must be publicly available to any wireless carrier.

Third, the Order defined limits on permitting fees and on recurring annual pole attachment revenues for small cell, or 5G, attachments to support smart city initiatives. For permitting fees, the Order set a minimum fee of $500 for an application of up to five (5) poles, with an additional $100 per each additional pole. (For the fee discussion, poles may be defined as streetlights, traffic lights, or any other municipally owned asset.)

For recurring annual pole attachment fees, the Order is much more interesting. It sets a safe harbor rate of $270 per pole per year as a safe harbor which cannot be challenged. However, that can be seen as a safe floor rate. The Order indicates that a jurisdiction could justify a higher pole revenue fee if the direct costs of maintaining the set of poles is documented and can be shown to be higher. Nothing in the Order precludes negotiating a higher annual rate, mutually acceptable to both Chula Vista and the carrier. In fact, the carrier's only recourses in the event it perceives the rates are too high are to:

- Walk away from the municipality – which seems in conflict with carrier's desire to enter the City; or
- Bring suit against the municipality – which brings all the costs and adverse optics of a carrier wishing to do smart city business.

Neither option seems likely. There is consequently some pricing flexibility above the $270 per pole per year recurring rate. The path of least resistance might be the $270 rate, however.

Finally, there had been concern that the Order would void existing agreements in place for recurring annual fees, such as the ones Chula Vista has in place with Mobilitie. However, the Order did not address any existing agreements and so those remain in force. The lack of voiding agreements was unsurprising as these are typically agreements between two parties (the municipality and the wireless carrier) and the FCC did not intend to involve itself with all these private agreements.

16. Magellan Advisors' Disclaimers

Magellan Advisors' Legal Disclaimer

This report (including any enclosures and attachments) has been prepared for the exclusive use and benefit of the Client and solely for the purpose for which it is provided. Unless Magellan Advisors provides express prior written consent, no part of this report may be reproduced, distributed or communicated to any third party. Magellan Advisors does not accept any liability if this Report is used for an alternative purpose from which it is intended, nor to any third party in respect of this report.

These materials have been prepared for informational purposes only and concern hypothetical and/or historical situations. The information is not intended as and should not be construed to provide any legal advice as Magellan Advisors does not provide legal services. Magellan Advisors and its directors, employees, contractors or associates shall not be liable for any direct or indirect consequential loss suffered by any person or organization as a result of using or relying on any statement in or omission from this Report (including any enclosures and attachments).

Magellan Advisors' Disclaimer on Financial Information, Assumptions, Forecasts and Risks

Magellan Advisors' financial models, estimates, forecasts and related financial and business risk analyses have been prepared for use solely by Magellan's Client in understanding the financial aspects of proposed broadband and telecommunications projects. Magellan accepts no responsibility or liability towards any third party in respect of this information or related content in this Report. This information is subjective in many respects, and, thus, susceptible to multiple interpretations and periodic revisions based on actual experience and business developments.

The financial information contained in this Report contains a significant number of subjective forecast assumptions including, but not limited to, subscriber take rates, rate structures, fixed and variable costs, costs of capital and related assumptions. Any deviation from the subjective forecast assumptions is likely to lead to results that are significantly different than those projected in the Report. Additionally, other events that are not explicitly allowed for in the Report and financial analysis may lead to significantly different returns or values.

Neither the financial information contained herein nor its outputs necessarily represent the opinion of value or future investment returns that are achievable. The financial information prepared by Magellan Advisors in this Report is provided for the sole purpose of indicative results based on a given set of assumptions. Neither Magellan Advisors itself, nor its directors, employees, contractors or associates shall be liable for any direct or indirect consequential loss suffered by any person or organization as a result of using or relying on any statement in or omission from this financial information or any information provided in connection herewith.

Appendix A – Dig Once Policy, Including Joint Trench

PURPOSE:

The purposes of implementing a Dig Once policy include:

- Protecting newly and recently paved roads and sidewalks
- Ensuring efficient, non-duplicative placement of infrastructure in the Public Rights of Way (PROW)
- Minimizing the impact of construction on residential and commercial communities
- Reducing overall costs of all underground work in the PROW by capitalizing on significant economies of scale
- Enhancing the uniformity of construction
- Leveraging construction for the deployment of a public communications network

BACKGROUND:

Encouraging simultaneous underground construction and co-location of infrastructure in the PROW creates benefits both the community and all users of the PROW. The excavation of roads and cutting of sidewalks substantially reduces the lifetime and performance of those surfaces. Furthermore, each excavation diminishes the space available for future infrastructure. While aerial construction methods requiring attachments to utility poles are usually less expensive than underground construction, aerial installation have significant drawbacks, including a limit to the quantity of cables and attachments that can be placed on existing utility poles in more crowded areas, lack of ownership of overhead infrastructure, and greater exposure to outside conditions. Underground construction, using protective conduit, generally provides scalable, flexible, and durable long-term infrastructure.

POLICY DIRECTIVE:

1. Unless waived by the Public Works Director because of undue burden, or an unfavorable cost-benefit analysis, or the consideration of other relevant factors, the PROW Excavator/Permittee will install two 3-inch diameter conduits for the following types of projects that has a minimum continuous open trench length of 300 feet:
   a) Excavations for the purpose of installing utilities, including but not limited to communications, electrical, gas, water, wastewater, storm drainage.
   b) Other excavations, or work on public property or in the public right of way that provide a similar opportunity to install conduit for future use.
2. Unless the Public Works Director determines otherwise, the typical standard installation requirements are listed below:
   a) Pipe diameter 3-inch nominal.

b) Made of PVC Schedule 40 material.
c) Laid to a depth of not less than 18 inches below grade in concrete sidewalk areas, and not less than 24 inches below finished grade in all other areas when feasible, or the maximum feasible depth otherwise.
d) When feasible and needed, install minimum 3-foot radius sweeps and bends.
e) When practicable, furnish with 10 AWG insulated tracer wire inside at least one pipe and an external "warning" ribbon tape a minimum of 3-inches above the conduit.
f) All conduit couplers and fittings shall be installed to be watertight. Conduits shall be sealed with endcaps upon installation.

3. Conduits installed will be owned by the City.
4. A record of all City-owned conduits will be documented and transferred to the City for geographic information system (GIS) entry whenever feasible.
5. The PROW Excavator/Permittee should make a documented effort to work with other utility agencies co-locate infrastructure in same trench whenever feasible to minimize construction costs, minimize future public disruptions and encourage efficient use of the PROW.
6. Each utility shall participate in periodic coordination meetings as requested by the City with other utilities and affected public agencies. The purpose of these meetings shall be to coordinate activity between public works projects and utility projects in the PROW.

Effective Date: TBD

Appendix B – Data Center Support

This Appendix enumerates the minimum data required to be managed to provide the controls enumerated in Section 3, "Data Center"

B.1 Environmental Controls

Objective: An organization should implement critical supporting utilities, such as climate control, fire suppressants and backup power supplies needed to support the business.

Risk Statement: The absence of environmental controls may result in the organization being more susceptible to business interruptions.

Control: Facilities housing scoped data, scoped systems and or physical media are protected with environmental controls.

B.1 ENVIRONMENTAL CONTROLS	Details
General Perimeter:	
Climate control system	
Thermostat sensor	
Raised floor	
Smoke detector	
Heat detector	
Fluid or water sensor	
Fire suppression system	
Uninterruptible Power Supply (UPS)	
Battery	
Generator	
Remote Monitoring	
Secure Perimeter:	
Climate control system	
Thermostat sensor	
Raised floor	
Smoke detector	
Heat detector	
Fluid or water sensor	
Fire suppression system	
Uninterruptible Power Supply (UPS)	
Battery	
Generator	
Remote Monitoring	

B.2 Physical Security Controls

Objective: An organization should ensure that physical access to data or systems is restricted by layered security controls and that only authorized personnel are allowed access to restricted areas.

Risk Statement: An organization should ensure that physical access to data or systems is restricted by layered security controls and that only authorized personnel are allowed access to restricted areas.

Control: Facilities housing scoped data, scoped systems and physical media are protected with physical security controls.

B.2 PHYSICAL SECURITY CONTROLS	**Details**
Immediate Perimeter:	
Camera to monitor physical access to immediate perimeter	
Badge, biometric readers or locked doors requiring a key or PIN on all points of entry	
Access logs	
Alarm system (motion, infrared or other detection mechanism for unauthorized entry)	
Cage or walls that completely enclose the immediate perimeter	
Secure Perimeter:	
Alarm system (motion, infrared or other detection mechanism for unauthorized entry)	
Mounted camera at points of entry	
Anti-tailgating/anti-piggybacking mechanisms at each point of entry	
Walls extend from true floor to true ceiling	
Security guards at each unlocked point of entry	
Badge, biometric readers or locked doors requiring a key or PIN on all points of entry	
Access Logs	
General Perimeter:	
Mounted camera at points of entry	
Anti-tailgating/anti-piggybacking mechanisms at each point of entry	
Security guards at each unlocked point of entry	
Badge, biometric readers or locked doors requiring a key or PIN on all points of entry	

B.2 PHYSICAL SECURITY CONTROLS	Details
Access Logs	
External Perimeter:	
Defined boundary or property line	
Physical barrier	
Signage identifying the facility as a data center is not present	
Mounted camera at points of entry	
Anti-tailgating/anti-piggybacking mechanisms at each point of entry	
Security guards at each unlocked point of entry	
Badge, biometric readers or locked doors requiring a key or PIN on all points of entry	
Access logs	
Obtain from the organization CCTV images from the past 30 days, and report if images requested are present	
Inspect the constituents you come in contact with for evidence of photo ID badge being visibly displayed on constituents while within company facilities	
Number of constituents where photo badge is not present	

B.3 Secure Workspace Program

Objective: An organization should ensure that protecting the secure workspace environment is part of the physical security and risk management programs.

Risk Statement: The absence of a secure workspace program may result in the organization's inability to identify appropriate procedures to secure the workspace environment.

Control: A formal enterprise risk governance program is aligned with the business environment and organizational strategic objectives.

B.3 SECURE WORKSPACE PROGRAMS	Details
Electronic writing instruments	
Cell phones, PDAs or smartphones	
Cameras	
Personal recording devices	
Printing privileges limited to persons with a role-based need to print	
Internet access limited for business	
Policy prohibiting automatic updates	

B.3 SECURE WORKSPACE PROGRAMS	Details
Provisions for prohibiting peer-to-peer user networking	
Provisions for the secure disposal of scoped data	
Provisions for the secure storage of scoped data	
Process to escalate security issues	
Prohibition of external instant messaging	
Prohibition of employees and contractors accessing public external email servers	
Prohibition of auto-forwarding of emails	
Prohibiting transmission of scoped data	
Policy outlining clean desk and screen lock parameters	
Approver's title	
Date of last approval	
Date of last policy review	

B.4 Secure Workspace Perimeter

Objective: An organization should control ingress and egress to/from the secure workspace. The level of controls should be commensurate with the level of risk.

Risk Statement: The absence of a secure workspace perimeter may result in the organization being more susceptible to unauthorized access to facilities housing scoped data, systems or media.

Control: Organizations have implemented physical security control features to control ingress to and egress from the secure workspace.

B.4 SECURE WORKSPACE PERIMETER	Details
Entry points:	
Mounted camera	
Anti-tailgating (anti-piggybacking) mechanisms	
Security guards	
Locked door	
Badge, biometric reader, key or PIN required for access	
Walls that completely enclose the secure workspace	
Physical inspection of bags upon entrance	
Access log (physical or electronic)	
Exit points:	
Mounted camera	
Anti-tailgating (anti-piggybacking) mechanisms	
Security guards	

B.4 SECURE WORKSPACE PERIMETER	Details
Badge or PIN required for exit	
Walls that completely enclose the secure workspace	
Physical inspection of bags upon exit	
Emergency exit points:	
Mounted camera	
Signage identifying alarm	
Locked to prevent access from the outside in	
Walls that completely enclose the secure workspace	

B.5 Secure Workspace Access Reporting

Objective: An organization should maintain access reports.

Risk Statement: The absence of access logging management may result in the organization's inability to identify or report unauthorized access to secure workspaces.

Control: Access to secure workspace is logged and reports are maintained.

B.5 SECURE WORKPLACE ACCESS REPORTING	Details
Access logs:	
Name	
Date and time	
Point of access	
Company name	
Sponsor/point of contact	
Equipment	
Date of last update of incident and access logs	
Logs maintained for at least 90 days	

B.6 Secure Workspace Compliance Inspections

Objective: An organization should complete periodic compliance inspections of the secure workspace desktop environment.

Risk Statement: The absence of compliance inspection for the secure workspace desktop environment may result in the organization's inability to identify ineffective practices, and loss or compromise of information or assets

Control: Periodic compliance inspections of the secure workspace environment are conducted.

B.6 SECURE WORKSPACE COMPLIANCE INSPECTIONS	Details
Inspection program:	
Requirement to inspect the secure workspace environment	
Role(s) responsible for inspection	
Inspection reports created and maintained	
Remediation action required on inspection findings	
Frequency of inspection	
Inspection results are reviewed as part of the organization's security and risk management program	
Inspect against a list of compliance checks which includes:	
Clean desk review	
External storage devices:	
Mobile devices	
Cameras	
Screen lock on unattended desktops	
Scoped data in common areas	
Scoped data on or near printers	
Inspection report:	
Title of inspector	
Date of inspection	
Inspection notes or findings	
Date of last inspection	
Frequency of inspections	

B.7 Visitor Management

Objective: An organization should establish a visitor management program.

Risk Statement: The absence of adequate visitor management procedures may result in unauthorized or unsupervised visitor access.

Control: An organization has a process in place for visitor's who visit the facility, which includes the visitor presenting a valid government issued ID and display of a visitor's badge at all times.

B.7 VISITOR MANAGEMENT	Details
Visitor management documentation:	
Visitor sign-in process	
Visitor escort process	

B.7 VISITOR MANAGEMENT	Details
Visitor exiting process	
Visitor's logs from the past 90 days:	
Evidence of visitor signing in	
Evidence of visitor signing out	
Observe a visitor check in for evidence of the following attributes:	
Requirement to present valid government issued photo ID	
Requirement to display a visitor's badge	

B.8 Business Resiliency

Objective: An organization should create and maintain in-depth business resiliency governance policy, function and processes that documents overall expectations for the program, how the program is to be executed and defines responsibility for each element of the program.

Risk Statement: The absence of a business resiliency governance policy to guide the risk management program may result in a lack of clear direction and senior management involvement to assure readiness to handle service disruptions and impact to the products and services provided by the organization.

Control: A formal policy is in place which establishes program objectives, responsibilities and processes.

B.8 BUSINESS RESILIENCY	Details
Individual Program owner	
Requirement for annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, risks and issues including:	
Resource commitments including people, technology, facilities, equipment, third party services and funding	
Reporting of key program activity and value metrics	
Results of Business Continuity Program audits and reviews, including key suppliers and partners as appropriate:	
Results of exercising and testing	
Lessons learned and actions arising from disruptive incidents	
Required and satisfied competencies for person(s) working within the Business Resiliency program	
Defined repository for all business resiliency related plans and reference information	

B.8 BUSINESS RESILIENCY	Details
History of changes and related approvals made to all business resiliency plans	
Indication that the in-scope products and/or services fall within the scope of the Business Resiliency program	
Requirement for periodic (at least annual) reviews of the following documents:	
Business Resiliency Policy	
Business Impact Analysis	
Risk Assessment	
Business Continuity Plans	
Disaster Recovery Plans	
Requirement for event-based reviews of Business Continuity and/or Disaster Recovery Plans based on major events or business changes including, but not limited to:	
Recommendations from independent reviews of plans and program	
Changes in business activities, dependencies and related recovery objectives	
Changes in organizational structure and personnel changes	
Emerging threats and identified new risks	
Warning and communication procedures and capabilities	
Updates from the inventory of IT and telecom assets	
Requirement for periodic (at least annual) identification of exercises to be undertaken over a defined planning horizon	
Report titles of the business resiliency governance body members	
Report the titles of those that were not present at the last meeting	
Frequency of meetings	
Dates of the last two meetings	

B.9 Business Impact Analysis

Objective: An organization should conduct an assessment to prioritize all business assets and activities, including their interdependencies, as part of a workflow analysis. This assessment should also evaluate the potential impact of business disruptions resulting from uncontrolled, non-specific events on the organization's business functions and activities.

Risk Statement: The absence of a business impact analysis may result in lack of prioritization of business assets and activities, which could in turn prevent the necessary assets and activities from being prepared to respond to a business disruption that impacts the continued availability of critical products and services.

Control: Business impact analysis is performed, maintained and reviewed by senior management, as well as exercised periodically (at the minimum, annually), and upon material changes to critical business functions and their required assets and dependencies.

B.9 BUSINESS IMPACT ANALYSIS	Details
Date of BIA completion or refresh within the past 12 months	
Business activity or process criticality ratings (i.e., high, medium or low; numerical rating) that distinguishes the relative importance of each activity or process	
Criticality ratings for cyber security related business activities or processes	
Identification of resource dependencies including applications, data, network services, equipment, facilities, third party services, personnel, supplies and paper documents necessary for business activity or process recovery	
Maximum acceptable outage / Maximum Tolerable Period of Disruption for each Business Activity or Business Process	
Recovery Time Objectives for critical and essential Resource dependencies including application systems, network services, third party services and other resources	
Recovery Point Objective for critical and essential resource dependencies including application systems, data, and content repositories	
Identification of the Information Technology infrastructure requirements supporting critical and essential application systems and network services	
Identification of capacity requirements for critical and essential resource dependencies necessary to address needs/expectations of all clients/customers	
Identification of the impact of an activity or process outage on clients/customers	
Date of the BIA	

B.10 Risk Assessment

Objective: An organization should create and maintain an in-depth business risk assessment that identifies and analyses the likelihood and impact of disruptive incidents to the organization and its clients/customers.

Risk Statement: The absence of a risk assessment program may lead to unidentified threats and treatments that result in business disruption.

Control: Risk assessments are performed, maintained and reviewed by senior management for the critical resource dependencies identified by the business impact analysis.

B.10 RISK ASSESSMENT	Details
Malicious threats:	
Fraud	
Theft	
Blackmail	
Sabotage	
Terrorism	
Network Penetration	
Natural threats:	
Floods or water damage	
Severe weather	
Infectious disease or pandemic outbreak	
Accidental threats:	
Fire	
Air contaminants	
Hazardous material release	
Business or IT activity error	
Technical failure threats:	
Hardware, software or equipment capacity component failure	
Hardware, software or equipment capacity shortage	
Cyber protection hardware, software or equipment failure or malfunction	
External action threats:	
Business environment	
Legal, regulatory or industry standard changes	
Customer contract changes and cancellations	
Asset types to include, but not limited to:	
People (health and safety)	
Information (electronic and paper)	
Software	
Hardware	

B.10 RISK ASSESSMENT	Details
Network	
Network control (firewalls, appliances)	
Facilities (power, utilities, physical access controls)	
Equipment (non-IT related)	
Third party goods and services	
Analysis of risks identified to include:	
Probability of occurrence	
Impact	
Relevance (if applicable)	
Determination of those risks requiring treatments.	
Defined actions and assigned responsibilities on approved treatments	
Identified business activity risks associated with the unavailability of systems, information, people, third parties and facilities	
Date of risk assessment	

B.11 Business Activity Level Recovery Planning

Objective: An organization should create business recovery plans that will effectively guide the recovery of the critical business activities identified from the BIA.

Risk Statement: The absence of formal business recovery plans may result in critical business activities not being recoverable within needed timeframes.

Control: Business recovery plans are developed, maintained and reviewed periodically (at the minimum, annually) by senior management.

B.11 BUSINESS ACTIVITY RECOVERY PLANNING	Details
Date of last review and update within the past 12 months.	
Specific business response and recovery strategies that address the unavailability of critical resources including reduction in available work force, unavailability of workplaces, unavailability of IT and communication services, loss of data, unavailability of third-party services.	
Specific technology architectures, strategies and capabilities in place to facilitate recovery of critical and essential application systems and network/infrastructure services that may include:	

B.11 BUSINESS ACTIVITY RECOVERY PLANNING	Details
Networks are fully redundant, with at least two network paths to any node, and for every network device, at least one other redundant network device of the same type	
There is sufficient redundancy capacity that services are not impacted in multi-tenancy environments during peak usage and above	
There is sufficient Volume or Disk partitioning to prevent inadvertent resource bottlenecks from guest operating systems	
Availability modes that are aligned with recovery objectives (e.g., systems with RTOs of 4 hours or less correlate to an active/active architecture)	
Action procedures or checklists to guide the initiation and execution of the defined response and recovery strategies	
Inclusion of or link to the reference information needed to undertake the defined action procedures	
Inclusion of information security and IT operations activities within the scope of the recovery plans	
Identification of who within the organization has approved the plans	
Identification of who within the organization has received or has access to the plans	
Conditions for activating the plans	
Roles and responsibilities for personnel who invoke and execute the plans	
Means of communication (primary and alternate) for designated recovery teams	
Procedures and authorities for notifying and sustaining communications with customers/clients that may be impacted by a business disruption	
Identified virtual, physical command centers where management can meet, organize and manage emergency operations	
Identified primary, alternate personnel to lead recovery efforts	
Identification of dependencies with third party providers to include:	
Documented contact information for key service provider personnel	
Within the past 6 months the contact information been reviewed and updated	

B.11 BUSINESS ACTIVITY RECOVERY PLANNING	Details
Procedures for incident notification and escalation	
Procedures for ongoing communication in the event of a disruption that impacts delivery of their products and services	
Processes implemented to notify the service provider when their Business Resiliency Procedures are modified	
A list of critical vendors or subcontractors and/or dependency chart(s) is available for customer/client review	
Within the past 12 months each necessary vendor or sub-contractors has provided evidence or attested to the fact that they can fully recover and resume services within acceptable timeframes following an IT disaster, information security incident, or an incident impacting their facilities or work force	
Priority access to resources from suppliers is contractually secured in the event of an adverse situation, affecting multiple customers of suppliers (e.g., fuel oil, recovery center space)	
Date of last review	
Title of reviewer	

B.12 Backup Media Restoration

Objective: An organization should have systems, applications and data available in the event of an incident that compromises its production information technology operations. Backups or replications of scoped data should be available to meet required Recovery Point Objectives. (RPO) and Recovery Time Objectives (RTO).

Risk Statement: The absence of processes and capabilities for the restoration of scoped data and software may lead to a loss of ability to resume operations and the provisioning of services in the event of corruption or loss of the primary data source.

Control: An organization has implemented a backup or replication process for its systems, applications and data in order to ensure successful restoration.

B.12 BACKUP MEDIA RESTORATION	Details
Specific technology architectures, strategies and capabilities in place to facilitate backup/replication and recovery of critical and essential data that may include:	
How data and software backups and replications are performed and monitored	
Schedule for taking backups / replicating data and for identification and resolution of errors	

B.12 BACKUP MEDIA RESTORATION	Details
Process for daily validation of accuracy, completeness and resolution of errors	
Process for backup logging	
Actions to be undertaken if there are exception alerts	
Retention, location, and periodic verification of backup media inventories and records of secured transport, verification of receipt and chain of custody	
Environmental storage requirements for backup media (onsite and offsite)	
Policy for backup of production data and it includes requirements for annual or more frequent testing of restoration procedures and capabilities	
Report the attributes listed that are not present and the frequency of restoration testing	
Obtain from the organization the list of backup media generated within the last six months	
From the list obtained, randomly select one item of onsite media that contains readable files such as a text file, document or spreadsheet, which is greater than 0k in size	
For the sample item selected, randomly select single readable file	
Observe a representative of the organization restore the selected file	
Report if file could not be restored, or if contents of file were corrupt	

B.13 Exercise Business Continuity, Disaster Recovery Tests

Objective: An organization should conduct thorough exercises that validate the effectiveness of business continuity and disaster recovery procedures and capabilities, the readiness of its personnel to perform required actions and the viability of related communication mechanisms and procedures.

Risk Statement: The absence of exercising and testing may lead to unprepared individuals, unanticipated delays in meeting recovery objectives, and/or unidentified gaps in the program.

Control: Business resiliency and disaster recovery exercises are defined, scheduled, planned, conducted and evaluated according to a consistent process. The problems identified are made visible and documented with an associated remediation action plan.

B.13 EXERCISE BUSINESS CONTINUITY, DISASTER RECOVERY TESTS	Details
Prior audit and/or regulatory examinations and recommendations	
Procedures for defining, planning, executing and evaluating exercises	
Business Continuity related exercise options defined for key disruption scenarios including:	
Unavailability of workplaces / buildings (e.g., work remotely, relocate to alternate workspace)	
Unavailability of work force (e.g., reallocate work across available personnel)	
Unavailability of IT Services (e.g., utilize alternative systems or manual means)	
Unavailability of Network (e.g., outreach to impacted customers)	
Unavailability of third-party service (e.g., utilize alternative third-party service provider)	
Disaster Recovery related exercise options defined for key disruption scenarios including:	
Loss of production data center (e.g., failover to DR site and operate)	
Loss of data stores (e.g., failover to replicated data stores)	
Loss of recovery supporting personnel (e.g., utilize third party for recovery support)	
Loss of network (e.g., failover to DR site and operate)	
Loss of individual application	
Cyber Resilience related exercise options defined for key disruption scenarios including:	
Malware	
Insider threats	
Data or systems destruction and corruption	
Communications infrastructure disruption	
Simultaneous attack concurrent with third party service provider	
Other exercise options, such as:	
Notification and Communication	
Joint with third party Service Provider	
Joint exercises with customers/clients	
Infectious disease / pandemic outbreak	
Recovery of information security controls that may be impacted by disaster event	
Severe weather	

B.13 EXERCISE BUSINESS CONTINUITY, DISASTER RECOVERY TESTS	Details
Evacuation	
Unexpected higher than normal service levels during times of wide-spread disaster (e.g. extra cash in automated teller machines; computer equipment in stock)	
Replenishment of consumable resources that will be needed during recovery (e.g., electric generator fuel)	
Recovery and continuity of information security operational processes and controls that may be impacted by a non-Disaster Recovery even	
Recovery and continuity of IT operational processes and controls that may be impacted by a non-Disaster Recovery event. Examine documentation for evidence of exercise types such as:	
Tabletop/walk-thru:	
Parallel processing/operations	
Partial interruption / limited scale	
Complete interruption / full scale	
Typical business volumes / full capacity (daily, weekly, etc.)	
Inspect the exercise specific documentation obtained for evidence of the following attributes:	
Observable and measurable exercise objectives	
Defined exercise scope to include specific capabilities and dependencies that have been excluded from scope	
Prior exercise results	
Formal statement of changes in business operations and/or information technology (external and internal) since the last similar scope exercise	
Exercise Results and Actions:	
Outcomes linked to stated exercise objectives	
Root cause and lessons learned	
Action/remediation plans have been identified for remediation and communicated within the organization	
Action/remediation plans that have been shared with customers/clients	
If exercise related procedures are present, report the following:	
Procedures have been reviewed by a third party and/or an internal auditor	
Date of last review and update	

B.13 EXERCISE BUSINESS CONTINUITY, DISASTER RECOVERY TESTS	Details
Name of the member of management who performed or oversaw the review	
Revision history is not present	
Report the name of the business activity sampled or the nonexistence of business resiliency exercise procedures	

B.14 Infectious Disease Planning

Objective: An organization should create and maintain infectious disease outbreak plans which consider outbreaks impacting internal parties, third parties and customers.

Risk Statement: The absence of formalized process to respond to infectious outbreaks could result in the inability of the organization to continue to provide its products, services and related support or to adapt to changes in demand by its customers impacted by an outbreak.

Control: An infectious disease plan is established to define how the organization will prepare for and respond to the pandemic and epidemic outbreaks that may or do impact the organization, its personnel and ongoing operations.

B.14 INFECTIOUS DISEASE PLANNING	Details
Types of infectious diseases (e.g., influenza pandemic, Ebola, measles) to which the plan relates	
Action plans to reduce the likelihood and impact of outbreaks degrading the delivery or quality of products and services	
Action plans or strategies to address changes in customer demand for products, services and related support	
Inclusion of or link to the reference information needed to undertake the defined action procedures	
Identification of who within the organization has approved the plan	
Identification of who within the organization has received or has access to the plan	
Conditions for activating the plan	
Roles and responsibilities for personnel who execute the plan	
A defined exercise regime/schedule focused on key elements of the plan	
A date of last review and update within the past 12 months	
Name of management member who performed last review or if revision history is not present.	
Date of last review	

B.14 INFECTIOUS DISEASE PLANNING	Details

B.15 Business Insurance

Objective: An organization should ensure all applicable insurance coverage(s) is defined and outlined within their business resiliency plan.

Risk Statement: The absence of insurance could result in a financial loss to the company putting at risk their ability to resume services to their customers in a timely manner.

Control: Insurance coverages held by the organization are defined and outlined within their business resiliency plan.

B.15 BUSINESS INSURANCE	Details
Scope of coverage that includes all goods and services received from the third party	
Carrier	
Policy Number	
Policy Expiration Date	
Agent Name	
Agent Contact Information	

Appendix C – List of City Sites

This Appendix lists all twenty-six City sites to be connected to the Rings. It also includes park and recreation center sites which may be optionally connected later.

Figure C-1 City Sites and Lateral Priority 1

Site Name	Street Address	Priority	Phase
Public Works (Data Center)	1800 Maxwell Rd	1	1
Civic Center Bldg A (City Hall Data Center)	276 4th Avenue	1	1
Police Department (Data Center)	315 4th Avenue	1	1
Civic Center Bldg B (Traffic Mgmt Center)	276 4th Avenue	1	1
Civic Center Bldg C	276 4th Avenue	1	3
Civic Library	365 F Street	2	3
South Library	389 Orange Avenue	2	3
Animal Control	130 Beyer Way	3	3
Boys and Girls Club of Chula Vista	1301 Oleander Av	3	3
Fire Station #3	1410 Brandywine Ave	3	3
Fire Station #9	266 E Oneida St	3	3
Chula Vista Women's Club	357 G Street	3	3
Fire Station #5	391 Oxford Street	3	3
Bonita Public Safety Center	4180 Bonita Rd	3	3
South Bay Community Services	430 F St	3	3
Fire Station #1	447 F St	3	3
Chula Vista Community Youth Center	465 L St	3	3
Chula Vista Harbor	550 Marina Pw	3	3
Visitor Information Center	750 E Street	3	3
Fire Station #2	80 East J St	3	3
Fire Station #8	1180 Woods Dr	3	4
Fire Station #7	1640 Santa Venetia St	3	4
Otay Ranch Community Storefront	2015 Birch Rd	3	4
Olympic Training Center	2800 Olympic Pkwy	3	4
Fire Station #6	605 Mount Miguel Rd	3	4
Fire Station #10 (Future)	610 Bay Blvd	3	4
Fire Station #4	850 Paseo Ranchero	3	4
Chula Vista Community Park	1060 Eastlake Pkwy	3	N/A
Breezewood Park	1091 Breezewood Drive	3	N/A
Voyager Park	1178 E J Street	3	N/A
Greg Rogers Park	1189 Oleander Av	3	N/A
Independence Park	1248 Calle Santiago	3	N/A
Rancho Del Rey Park	1311 Buena Vista Way	3	N/A
Palomar Park	1359 Park Drive	3	N/A
Santa Cora Park	1365 Santa Cora	3	N/A
Heritage Park & Recreation Center	1381 E Palomar Street	3	N/A
Sunset View Park	1390 S Greensview Drive	3	N/A

Loma Verde Aquatic Park & Rec. Center	1420 Loma Ln	3	N/A
SDG&E Park	1450 Hilltop Drive	3	N/A
Orange Park	1475 Fourth Ave	3	N/A
Mountain Hawk Park	1475 Lake Crest Drive	3	N/A
Los Ninos Park	150 Teal Street	3	N/A
Santa Venetia Park	1500 Magdalena Ave	3	N/A
Rienstra Sports Complex	1500 Max Ave	3	N/A
Montecito Park	1501 Santa Diana Road	3	N/A
Harvest Park	1550 E Palomar Street	3	N/A
Connoley Park	1559 Connoley Ave	3	N/A
Otay Park	1613 Albany Ave	3	N/A
Windingwalk Park	1675 Exploration Falls Drive	3	N/A
Tiffany Park	1713 Elmhurst Ave	3	N/A
Bonita Long Canyon Park	1745 Coltridge Lane	3	N/A
Cottonwood Park	1778 E Palomar Street	3	N/A
All Seasons Park	1825 Magdalena Avenue	3	N/A
Stylus Park	2025 Stylus Street	3	N/A
Mount San Miguel Park	2335 Paseo Veracruz	3	N/A
Norman Park / Senior Center	270 F St	3	N/A
Salt Creek Park & Recreation Center	2710 Otay Lakes Rd	3	N/A
Eucalyptus Park Ball/Sports Fields	276 4th Av & C Street	3	N/A
MacKenzie Creek Park	2775 Mackenzie Creek Rd	3	N/A
Lauderbach Park	333 Oxford Street	3	N/A
Otay Recreation Center	3554 Main Street	3	N/A
Memorial Bowl / Park	373 Park Way	3	N/A
Parkway Aquatic/Community Center	373 Park Way	3	N/A
Holiday Estates I & II Park	383 Connoley Circle	3	N/A
Gayle L. McCandliss Park	415 E J Street	3	N/A
Terra Nova Park	450 Hidden Vista Drive	3	N/A
Rohr Park	4548 Sweetwater Road	3	N/A
Friendship Park	4th Av & F Street	3	N/A
Sunbow Park	500 E Naples Street	3	N/A
Valle Lindo Park	545 Sequoia Drive	3	N/A
Harborside Park	670 Oxford Street	3	N/A
Sherwood Park	69 Sherwood Street	3	N/A
Discovery Park	700 Buena Vista Way	3	N/A
Lancerlot Park	750 K Street	3	N/A
Paseo Del Rey Park	750 Paseo Del Rey	3	N/A
Hilltop Park	780 Hilltop Drive	3	N/A
Veterans Park & Recreation Center	785 E Palomar Street	3	N/A
J St Marina Bayside Park	800 Marina Pkwy	3	N/A
Montevalle Park & Recreation Ctr.	840 Duncan Ranch Rd	3	N/A
Marisol Park	916 Rancho Del Rey Pkwy	3	N/A
Sunridge Park	952 Beechglen	3	N/A
Horizon Park	970 E Palomar Street	3	N/A

Bay Boulevard Park	F Street & Bay Blvd.	3	N/A
Explorer Park	Rancho Del Rey Pkwy & Norella St	3	N/A

Appendix D – Financial Analysis for Chula Vista

The following chart summarizes the capital spending required for construction of the three rings, over six phases, connecting the 27 sites and several traffic signals. Capital spending also includes equipment refreshes in years 7 and 14, at approximately 50% of the original equipment expenditure, due to anticipated improved price / performance ratios.

Figure D-1 Annual Capital Spending