McDermott
Will & Emery

Boston Brussels Chicago Düsseldorf London Los Angeles Miami Munich
New York Orange County Rome San Diego Silicon Valley Washington, D.C.

Christine M. Gill
Attorney at Law
cgill@mwe.com
202.756.8283

October 12, 2006

VIA ELECTRONIC SUBMISSION

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

Re: *Ex Parte* Presentation; ET Docket No. 05-247

Dear Ms. Dortch:

On behalf of The Massachusetts Port Authority ("Massport"), this provides for inclusion in the record a proposal submitted to Massport by T-Mobile USA, Inc. prior to the installation of the central Wi-Fi antenna system at Boston-Logan International Airport.

On July 3, 2003, Massport issued a Request for Competitive Proposals for a high-speed wireless network system at Logan Airport. In response to this Request, T-Mobile submitted the attached proposal to "design, install, manage, operate, and maintain" a Wi-Fi network for use by the traveling public, Massport, airlines, and other tenants.

In Section 8.7.1.9 of the proposal, T-Mobile acknowledged the risk of interference to the Wi-Fi system. Although T-Mobile has repeatedly stated in this proceeding that Massport cannot prohibit tenants from installing antennas for use with unlicensed devices, this Section specifically "recommended that Massport enforce a wireless policy that restricts the placement of devices in said frequencies" to prevent interference at Logan.

We trust that this information will be of assistance in the FCC's further consideration of the issues in the above-referenced proceeding.

Very truly yours,

Christine M. Gill

Christine M. Gill

Enclosure

cc: Chairman Kevin J. Martin
Commissioner Michael J. Copps
Commissioner Jonathan S. Adelstein
Commissioner Deborah Taylor Tate
Commissioner Robert M. McDowell
Fred Campbell
Bruce Gottlieb
Aaron Goldberger
Angela Giancarlo
Barry Ohlson

# PROPOSAL

## HIGH SPEED WIRELESS NETWORK SYSTEM

SUBMITTED TO

MASSACHUSETTS PORT AUTHORITY

FOR

BOSTON-LOGAN INTERNATIONAL AIRPORT

**Submitted By:**

**T-Mobile USA, Inc.**

**August 15, 2003**

T-Mobile HotSpot

August 14, 2003

Ms. Leonor Filipe
Deputy Director of Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, Massachusetts, 02128-2909

Re: Request for Proposals – High Speed Wireless Network System

Dear Ms. Filipe:

T-Mobile is pleased to present the enclosed proposal to design, deploy and operate a High Speed Wireless Network System (HiWi) at Boston-Logan International Airport.

The proposal is organized to meet the needs expressed by Massport and is also founded upon our experience as the largest operator of WLAN Hot Spots (networks) in the United States.

T-Mobile looks forward to the opportunity to be a part of Massport's dynamic future and we appreciate the opportunity you have afforded us to play a role in providing solutions that will enrich the experience of BOS' passengers, tenants, and administrative personnel.

Sincerely,

Michael Allen
Manager, Aviation Site Services

massport

**REQUEST FOR COMPETITIVE PROPOSALS**
**BOSTON LOGAN INTERNATIONAL AIRPORT**

**HIGH SPEED WIRELESS NETWORK SYSTEM**

## III. PROPOSAL FORM

To: Massachusetts Port Authority
Logan Office Center
One Harborside Drive, Suite 200S
East Boston, Massachusetts 02128-2909

Attn: Ms. Leonor M. Filipe
Deputy Director of Information Technology

**T-Mobile USA, Inc.** (Name of Proposer) acknowledges receipt of Massport's Request for Competitive Proposals for the High Speed Wireless Network System, dated July 03, 2003, and hereby submits the following proposal in response thereto.

# PROPOSAL

## HIGH SPEED WIRELESS NETWORK SYSTEM

**SUBMITTED TO**

**MASSACHUSETTS PORT AUTHORITY**

**FOR**

**BOSTON-LOGAN INTERNATIONAL AIRPORT**

**Submitted By:**

**T-Mobile USA, Inc.**

T-Mobile HotSpot

**August 15, 2003**

## Table of Contents


1.0 Executive Summary ..... 1

1.1 Network Infrastructure ..... 1

1.2 Revenue Sharing ..... 1

1.3 Marketing ..... 2

1.4 Administrative & Reporting ..... 2

1.5 Neutral Host ..... 2

1.6 Project & Site Management ..... 2

1.7 Private Sector Services ..... 2

1.8 Billing, Customer Care, Network Monitoring, and AAA ..... 3

1.9 Massport Benefits ..... 3

2.0 T-Mobile and Sub-Contractors' Background ..... 3

2.1 T-Mobile Overview ..... 3

2.2 Hewlett-Packard Overview ..... 4

2.3 Syntegra Overview ..... 4

2.4 High-Speed Wireless Data Services ..... 4

2.4.1 Ubiquitous GSM/GPRS Voice/Data Network ..... 4

2.4.2 Wi-Fi HotSpots ..... 4

2.4.3 Current Airport HotSpot Locations ..... 5

2.4.4 Pending International Airport HotSpot Locations ..... 5

3.0 Operating Experience ..... 5

3.1 T-Mobile Operating Experience Overview ..... 5

3.2 Hewlett-Packard Operating Experience Overview ..... 6

3.3 Syntegra Operating Experience Overview ..... 6

3.4 Services Provider ..... 6

3.5 Relevant Projects..... 6

3.5.1 San Francisco International Airport – SFO..... 6

3.5.2 Dallas-Fort Worth International Airport – DFW..... 7

3.5.3 T.F. Green (Providence, RI) – PVD..... 7

3.5.4 Airline Clubs..... 7

3.5.4.1 Delta Airlines..... 7

3.5.4.2 American Airlines..... 8

4.0 Financial Proposal..... 8

4.1 Compensation..... 8

4.1.1 Revenue Sharing Percentages..... 8

4.1.2 Minimum Annual Guarantee (MAG)..... 8

4.1.3 Marketing..... 8

4.2 Data Capture..... 9

4.3 Other..... 9

5.0 Project Schedule..... 9

5.1 Project Schedule Assumptions..... 9

6.0 Management & Staffing Plan..... 9

6.1 Organizational Structure & Staffing Levels..... 9

6.1.1 Account Management..... 10

6.1.2 Program and Project Management..... 10

6.1.3 Engineering..... 10

6.1.4 Information Technology..... 10

6.1.5 NOC..... 10

6.1.6 Customer Care..... 10

6.2 Resumes – Key Personnel..... 10

7.0 Operation..... 10

7.1 Overview..... 10

7.2 Network Management Systems..... 11

7.3 Trouble Tracking and Issue Resolution Process..... 11

7.4 Moves, Adds, and Changes..... 12

7.5 Network Reliability, Reporting and Notification..... 12

7.6 Scheduled Maintenance..... 13

7.7 Field Service..... 13

7.8 Customer Care..... 13

8.0 Technical Proposal..... 14

8.1 Overview (a)..... 14

8.1.1 Quality Assurance Plan..... 15

8.1.2 Facilities and Utilities..... 15

8.1.3 Y2K Compliance..... 16

8.1.4 Inter-modulation Study..... 16

8.2 Radio Frequency Survey (b)..... 16

8.2.1 Access Point Placement and Interference Detection..... 16

8.2.2 Cabling / Fiber Paths..... 16

8.2.3 Primary Equipment Placement..... 16

8.2.4 Survey Documentation..... 17

8.3 Network (c)..... 17

8.3.1 Network Design..... 17

8.3.2 Redundancy..... 18

8.3.3 Security..... 18

8.3.4 Standards..... 18

8.4 Usage Monitoring & Reporting (d)..... 18

8.5 Access Control (e) ..... 19

8.5.1 Standards ..... 19

8.5.2 Roaming Access ..... 19

8.5.3 Open Access Tenant Access ..... 19

8.5.4 Private Access ..... 19

8.6 System Expansion Capability (f) ..... 19

8.7 Detailed Technical Requirements (g) ..... 19

8.7.1 Technical Requirements ..... 19

8.7.1.1 System Expandability ..... 19

8.7.1.1.1 Expandability – Capacity ..... 20

8.7.1.1.2 Expandability – New Network Components ..... 20

8.7.1.1.3 Expandability – Emerging Technologies ..... 20

8.7.1.2 System Integration into the Airport Network ..... 20

8.7.1.3 Operational Requirements ..... 21

8.7.1.3.1 Compliance ..... 21

8.7.1.3.2 Seamless Coverage ..... 21

8.7.1.3.3 Capacity ..... 21

8.7.1.3.4 FHSS & DSS ..... 21

8.7.1.3.5 Channel Assignments ..... 22

8.7.1.3.6 Transmitter Power Output ..... 22

8.7.1.3.7 Integration with Airport-Wide Wireless LAN System ..... 22

8.7.1.3.8 Collection of System Usage Data ..... 22

8.7.1.3.9 Operating, Maintaining, and Upgrading ..... 22

8.7.1.4 Interoperability ..... 23

8.7.1.5 Site Survey ..... 23

8.7.1.6 Coverage Areas..... 23

8.7.1.7 Location of Access Points..... 23

8.7.1.8 Load Balancing..... 23

8.7.1.9 RF Interference..... 23

8.7.1.10 Network Security..... 24

8.7.1.10.1 Public WLAN..... 24

8.7.1.10.2 Private WLAN..... 24

8.7.1.11 Vendor Specific Solution..... 25

8.7.1.12 System Performance..... 25

8.7.1.13 Central Monitoring..... 25

8.7.2 Hardware Requirements..... 25

8.7.2.1 Materials..... 25

8.7.2.2 Wireless Network System Equipment..... 25

8.7.2.3 Hardware..... 25

8.7.2.3.1 Access Points..... 25

8.7.2.3.2 Antennae..... 25

8.7.2.3.3 Zone Controllers..... 25

8.7.2.3.4 Network Equipment..... 25

8.7.2.3.5 Special Equipment..... 26

8.7.2.3.6 Spares..... 26

8.7.2.4 Year 2000 Compliance..... 26

8.7.2.5 Power Source..... 26

8.7.3 Installation Requirements..... 26

8.7.3.1 Submittals..... 26

8.7.3.2 Hardware Installation..... 26

8.7.3.3 Software..... 26

8.7.3.4 Cable Installation..... 26

8.7.3.5 Cable Routes/Management..... 26

8.7.3.6 Shared Infrastructure..... 27

8.7.3.7 System Configuration Documentation..... 27

8.7.4 Acceptance Testing Requirements..... 27

8.7.4.1 Inspection..... 27

8.7.4.2 Site Acceptance Test..... 27

8.7.4.3 Operator Certification..... 27

8.8 Other (h) ..... 27

8.8.1 Expected Schedule..... 27

9.0 Administration & Reporting Plans..... 27

10.0 Confidentiality & Regulatory Matters..... 27

11.0 Contract Issues..... 28

11.1 Service Level..... 29

12.0 Non-Discrimination & Affirmative Action..... 29

12.1 Affirmative Action Plan..... 29

Attachment 1 – Hewlett-Packard Overview

Attachment 2 – Syntegra Overview

Attachment 3 – Project Schedule

Attachment 4 - Resumes

Attachment 5 – NOC Reports

Attachment 6 – Customer Care Reports

Attachment 7 – T-Mobile Generic Architecture

Attachment 8 – Redundancy in Preliminary Architecture

Attachment 9 – User Experience Screens

Attachment 10 – Usage Report

Attachment 11 – Hardware

Attachment 12 – Summary of Vendor's Estimated Expenses

Attachment 13 – Proforma

Attachment 14 – T-Mobile Reference Letters

Attachment 15 – T-Mobile Credit References

Attachment 16 - Appendix K – Proposer Information Form T-Mobile

Attachment 17 – Appendix K- Hewlett-Packard

Attachment 18 – Appendix K- Syntegra

Attachment 19 – Appendix M – T-Mobile, Workforce Composition Form

Attachment 20 – Appendix M –Syntegra, Workforce Composition Form.

Attachment 21 – Appendix M – Hewlett-Packard, Workforce Composition Form

Attachment 22 – T-Mobile Financial Reports

Attachment 23 – Hewlett-Packard Financial Reports

## 1.0 EXECUTIVE SUMMARY

Boston-Logan International Airport ("BOS") currently enjoys a leadership position among airports, being ranked as the 21st busiest in the United States and 37th in the world. The Massachusetts Port Authority (Massport) recognizes that with BOS serving approximately 22.7 million passengers annually, significant opportunity exists to further BOS' leadership position through the installation and operation of a state-of-the-art High Speed Wireless Network System (HiWi) that will accommodate a variety of applications and wireless devices for use by its passengers, airlines, tenants and other authorized users.

T-Mobile is responding to Massport's desire to select a strategic partner who will install, manage, operate and maintain a Wireless Services Network at BOS. In combining WLAN with our voice and GPRS data capabilities, T-Mobile is able to offer the most comprehensive wireless voice and data/information services available today. As the leading provider of Wi-Fi service in the United States, our experience in the design, installation and management of WLAN systems is second to none.

Should T-Mobile be selected as Massport's strategic partner, our Operations and Deployment teams are ready and committed to initiate the HiWi Management Program from design to implementation and launch by or before the required timeline.

### 1.1 Network Infrastructure

- T-Mobile will design, install, manage, operate and maintain the Hi-Wi Network at its expense for the purpose of providing WLAN service to the traveling public and to private sectors (Massport, airlines and other tenants) at BOS.
- The network coverage area will include Terminals B, C, D, and the Amelia Earhart Terminal, as well as Terminal E and other areas that may be designated by Massport.
- The network infrastructure will provide the ability to support seamless coverage and hand-offs or in-progress wireless data communications to, from, or between inside and outside coverage areas of the various facilities.
- The network will be structured to ensure interoperability of various networking systems while mitigating interference to the maximum extent possible.
- The network will provide the capability to add capacity and support emerging technologies as markets or needs may develop.
- Network installation will be completed and operational by or before June 1st 2004.
- Ownership of all hardware installed during the term of the Agreement will transfer to Massport upon the expiration of the Agreement term.

### 1.2 Revenue Sharing

T-Mobile will pay to Massport the greater of a Minimum Annual Guarantee or a percent of Net Revenue. Revenue generated by T-Mobile within those airline clubs and lounges where T-Mobile has an agreement to provide service, will be addressed under separate agreement.

**Revenue Sharing Percentages**

- 10% of net revenue realized on Public Sector* service and access including roaming and reselling revenues generated by qualified carrier partners.
- 20% of net revenue realized on all private sector services and access.

**Minimum Annual Guarantee (MAG)**

| | |
|---|---|
| Year 1 - $45,000 | Option Year 1 - $100,000 |
| Year 2 - $45,000 | Option Year 2 - $110,000 |
| Year 3 - $55,000 | |
| Year 4 - $75,000 | |
| Year 5 - $90,000 | |

## 1.3 Marketing

Marketing within the airport at BOS will include multiple diorama placements in all terminals with the focus on raising awareness of the availability of public Wi-Fi service throughout the facility. T-Mobile will provide informational materials, at no cost to BOS, for placement in information booths, passenger walkways, food courts and other approved areas.

T-Mobile expects to spend approximately $275,000 on in-airport advertising at BOS during the first year of the agreement and in excess of $300,000 in subsequent years.

BOS will be featured on www.t-mobile.com/hotspot and receive value-added placement in T-Mobile HotSpot partner co-marketing, such as being listed as a HotSpot service location in the Intel Centrino national print campaign. T-Mobile also plans to continue and expand its current global and national Wi-Fi campaigns that include television and print advertising in markets around the world.

## 1.4 Administrative & Reporting

- T-Mobile will establish an administrative system to ensure accurate revenue accounting for Massport, T-Mobile, and other wireless service providers.
- A site performance report of network availability metrics will be produced and submitted to the Airport on a monthly basis.
- Real-time network status reports will be made available via the Massport partner interactive website.
- Proactive notification of any scheduled maintenance that has potential to impact subscriber service will be provided not less than 48 hours prior to the scheduled maintenance.
- Usage reports for each provider will be submitted monthly and reflect usage in the areas in which activity took place.

## 1.5 Neutral Host

- T-Mobile will negotiate in good faith with all WSPs that desire to provide service at the Airport.
- T-Mobile is currently in negotiations with a number of qualified WSPs to roam on to existing T-Mobile networks in various US airports and expects to reach agreements with these and other providers for the BOS network if selected by Massport.
- Copies of all new agreements with WSPs that will provide service at the Airport will be provided to the Authority, and T-Mobile will report on a quarterly basis all WSPs that have agreements with T-Mobile to provide service at the Airport.
- T-Mobile will report on a quarterly basis those WSPs that have requested to provide service but do not have an agreement with T-Mobile. Information will be provided the state of progress towards reaching an agreement or the reasons why an agreement could not be reached.

## 1.6 Project & Site Management

- T-Mobile will draw upon our highly experienced staff and key vendors such as Hewlett-Packard and Syntegra to establish a core team with responsibility for planning, design, installation, marketing, and management of the WLAN at BOS.
- Weekly meetings will be held between the T-Mobile project team and designated Massport team members during the installation phase of the project.
- T-Mobile will provide informal training for Massport users on the HiWi and its interface to their specific applications on multiple occasions through the course of the agreement.

## 1.7 Private Sector Services

Hewlett-Packard, acting as a sub-contractor to T-Mobile, will be responsible for the installation, management, and maintenance of the private network to be installed at BOS, for use by BOS' airlines, tenants and other approved users. Hewlett-Packard will provide all back office, billing, authentication and

customer support and will be responsible to T-Mobile for all such private network services. Under the direction of T-Mobile, Hewlett-Packard will rollout the private network as appropriate to meet demand and commitments to use the network for private applications.

### 1.8 Billing, Customer Care, Network Monitoring, and AAA

T-Mobile will provide all back office billing, authentication, NOC (Network Monitoring), and Customer Care for public sector customers as well as all necessary settlement and clearing-house functions for roaming and reseller WSPs utilizing the WLAN network.

### 1.9 Massport Benefits

We believe that Massport's selection of T-Mobile as their WLAN business partner will be a sound decision because:

- T-Mobile is committed to establishing a long-term strategic partnership with Massport.
- T-Mobile is the preeminent WLAN provider in the U.S., having the largest WLAN footprint with over 2700 HotSpot locations today and building to over 4000 by year-end 2003.
- T-Mobile has more direct experience in the design, construction, and operation of WLAN networks in public venues such as airports than any other service provider today, in addition to retail venues (i.e. Starbucks, Kinkos, Borders, etc.).
- T-Mobile has a rapidly expanding international footprint with over 60 HotSpots available in the UK today, 865 additional HotSpots planned in airports and other venues this year, and over 3000 HotSpots by the end of 2004.
- T-Mobile has an established subscriber base and will continue to drive user adoption via its footprint and existing cellular subscriber base, enabling Massport to get maximum value from the airport's network.
- T-Mobile, as a division of the world's 3rd largest Telecom, remains financially sound and committed to the future wireless (voice and data/information) needs of Massport as a partner of our global team.
- T-Mobile is the industry's leading customer service provider, with all levels of customer care and NOC monitoring performed in-house at our state-of-the-art facility in Carrollton, Texas, ensuring that Massport passengers will enjoy the richest and most reliable wireless customer service experience in the industry.

## 2.0 T-MOBILE and SUB-CONTRACTORS' BACKGROUNDS

### 2.1 T-Mobile Overview

T-Mobile USA, a nationwide wireless voice and data carrier is the wholly owned U.S. subsidiary of T-Mobile International, the wireless subsidiary of Deutsche Telekom AG (NYSE:DT). Deutsche Telekom's subsidiaries and affiliated companies provide wireless services to more than 81 million customers worldwide, making it one of the top 3 global wireless carriers in the world, and the first wireless communications company to offer service on both sides of the Atlantic with a single global brand name and a single digital technology standard - GSM (Global System for Mobile Communications).

Based in Bellevue, WA, T-Mobile USA is one of the fastest growing wireless service providers in the country, with over 20,000 employees dedicated to serving over 10 million customers. Unlike other U.S. wireless operators, T-Mobile's entire wireless network is based exclusively on the Global System for Mobile (GSM) communications technology platform. GSM is the most widely used digital standard worldwide, accounting for over 70 percent of the total digital wireless market. T-Mobile customers benefit from this global association by having the choice to use their same phone and same phone number when traveling internationally.

T-Mobile offers consumers and enterprise customers the most advanced mobile communications services available today including voice; two-way text messaging; high-speed GPRS (General Packet Radio Services) wireless data services; and the nation's largest Wi-Fi (802.11b) wireless broadband service.

## 2.2 Hewlett-Packard Overview

Hewlett-Packard Company (HP) is a leading provider of computing products, technologies, solutions, and services to consumers and business. The company's offerings span information technology (IT) infrastructure, personal computing and access devices, global services, and imaging and printing. HP's basic business purpose is to invent, engineer, and deliver technology solutions that drive business value, create social value, and improve the lives of customers.

With annual revenue of $73 billion (U.S.), HP ranks in the top ten on the Fortune 500 and is one of the world's two largest computer companies. A truly global enterprise, HP provides sales and services in 160 countries and does business in 43 currencies and 15 languages. Led by Chairman and CEO, Carly Fiorina, the company employs approximately 140,000 people worldwide. HP's corporate headquarters is located in Palo Alto, California.

Hewlett-Packard's merger with Compaq Computer Corporation in May 2002 heralded the start of a new chapter in the company's long and distinguished history. The merger united two strong companies that together offer unparalleled market leadership and world-class technology innovation.

HP's market leadership spans a broad range of solution areas. With a number-one market share ranking in several key IT product segments, HP holds a formidable competitive position that is unmatched in the industry. Additional Information regarding Hewlett-Packard may be found in Attachment 1.

## 2.3 Syntegra Overview

Syntegra (USA) Inc. (Syntegra) is a worldwide consulting and systems integration business focused on the quality architecture, implementation, and lifetime support of electronic commerce business solutions. As the North American arm of British Telecommunications plc, Syntegra (USA) Inc. is a world leader in designing and deploying wireless services. From Wireless Access Protocol (WAP) applications for mobile phones to multisite wireless LANs, Syntegra's depth and breadth of wireless knowledge and experience is unsurpassed. Syntegra has deployed over 30,000 wireless access points in more than 4,000 locations in the USA.

With customers in more than 50 countries, Syntegra has revenues of over $1 billion and employs more than 4,000 people worldwide. In the United States, Syntegra combines comprehensive services with specialized market expertise. Additional information regarding Syntegra may be found in Attachment 2.

## 2.4 High-Speed Wireless Data Services

### 2.4.1 Ubiquitous GSM/GPRS Voice/Data Network

GPRS (General Packet Radio Service) is an extension of the GSM network architecture and provides T-Mobile customers with wireless Internet access at speeds that rival or exceed standard dial-up wired solutions. T-Mobile wireless Internet is available across the entire T-Mobile USA network. Through a series of integrated devices, customers can remotely access the Internet, corporate and personal email, contacts and calendar and popular services like news and information updates, games, AOL® E-Mail and AOL® Instant Messenger™ (AIM®) service.

Integrated devices include GPRS enabled phones; PC Internet Cards; and the popular BlackBerry 5810tm wireless handheld e-mail solution with Integrated phone. T-Mobile was the first U.S. carrier to introduce the much-anticipated Microsoft® Windows® Powered Pocket PC 2002 Phone Edition.

### 2.4.2 Wi-Fi HotSpots

T-Mobile USA offers Wi-Fi (802.11b) wireless broadband Internet access in over 2700 convenient public 'HotSpot' locations such as airports, clubs for American, Delta and United Airlines, Borders Books & Music Stores, Kinko's, and select Starbucks Corporation's coffeehouses. T-Mobile is the exclusive provider of high-speed Internet access for Starbucks, with plans to rapidly build out and market the service in over 70 percent of all Starbucks company-operated locations in North America over the next two years. T-Mobile was also selected to be the exclusive provider of high-speed Internet access for Borders Book & Music Stores with a planned build out of 443 locations, and for Kinkos with a planned build out of approximately 1100 locations.

Unlike some other providers of Wi-Fi service, T-Mobile provides at least a full T1 connection to every location where its service is available. Using either a laptop or PDA that is Wi-Fi (802.11b) wirelessly-enabled, users have the speed and bandwidth to access and download large email attachments, watch a live webcast, or listen to streaming audio.

T-Mobile's strategic plan provides for continuous growth of the network. The network will grow to over 4,000 'HotSpot' locations by year-end 2003, and future plans also include developing an integrated 802.11b/GPRS data card and other handheld devices, that would enable customers to have seamless service between the two networks to best meet their wireless data needs.

### 2.4.3 Current Airport HotSpot Locations

T-Mobile is the leader in providing Wi-Fi services to airports and airlines with current agreements that provide full coverage at nine airports including DFW and SFO, airline specific concourse coverage at four additional airports, and American, Delta, and United Airlines' club coverage in 119 clubs at thirty-nine airports. T-Mobile enables the mobile business passenger the greatest opportunity to use wireless services in aviation venues.

### 2.4.4 Pending International Airport HotSpot Locations

T-Mobile UK is working with the British Air Authority for pilot installations at Heathrow and Gatwick. Also, it is significant to note that T-Mobile UK has recently launched approximately 60 Starbucks stores in the UK, while T-Mobile, Germany has announced an agreement with Starbucks to provide WLAN service in all Starbucks stores in Germany.

## 3.0 OPERATING EXPERIENCE

### 3.1 T-Mobile Operating Experience Overview

T-Mobile International (the direct parent of T-Mobile USA) has rolled out GPRS wireless data services (30-50 kbps) across all its networks and is evolving these networks to 3G technology (WCDMA in Europe, EDGE in the United States).

T-Mobile USA's network covers over 245 million people in over 8,300 cities. T-Mobile was the first wireless carrier to install a nationwide high-speed packet data network (GPRS) that mirrors its voice footprint. Dedicated to a high Quality of Service and uptime, T-Mobile has built its own coast-to-coast nationwide ATM backbone, to support both voice and data traffic. Consistent with its worldwide outlook, T-Mobile's voice customers can roam in over 95 countries with over 200 other operators. T-Mobile continues to expend a significant amount of capital to enhance its network capacity.

A natural offshoot of these "wide area wireless networks" is the addition of commercial WLAN networks and services. T-Mobile leverages its core competency in provisioning, billing, security, network architecture, build out, roaming, and open standards to deliver a superior, reliable network execution.

In January of 2002, T-Mobile closed the purchase of nearly all of the Wi-Fi assets of MobileStar Network Corporation (MobileStar) a Wi-Fi provider who had been operating a public Wi-Fi network since 1996

and had 688 hotspot locations. Many of MobileStar's experienced and talented employees joined T-Mobile and are solely dedicated to building out and operating T-Mobile's HotSpot network and service. Since the asset purchase, T-Mobile has operated the legacy MobileStar Wi-Fi network, added 2069 new Wi-Fi locations in the U.S, and will have at least 4000 locations by the end of 2003.

### 3.2 Hewlett-Packard Operating Experience Overview

HP has long been providing market-leading wireless and mobile computing products for federal, state and local governments, communities, and businesses. HP has time proven experience in delivering wireless LAN/WAN solutions globally to major airports. HP consultants have the knowledge and expertise in wired and wireless networking solutions, application migration and enhancement, and technology management and support.

Experience in an Airport Environment:

- **Major European Airport** - This Major European Airport has engaged HP Services to provide a wireless solution to support baggage applications and independent airline applications, as well as provide capacity and services for Public Wireless Access and Operations of the network
- **Major Canadian Airport** – This Major Canadian Airport has engaged HP Services to provide a wireless solution to support baggage applications and independent airline applications, as well as provide capacity and services for Public Wireless Access, Operations, and Help Desk for the network.

### 3.3 Syntegra Operating Experience Overview

Syntegra's WLAN capability is applicable across a wide range of industry sectors.
The following two examples of wireless projects testify to Syntegra's experience and capability with LAN infrastructure projects.

Syntegra was recently contracted to conduct a site survey for the initial phase of a wireless prescription tracking system rollout at St. Mary's Hospital of Madison, Wisconsin. St. Mary's new system will utilize a wireless business application from Bridge Medical Systems called MedPoint. MedPoint is the only Barcode-enabled Point-Of-Care (BPOC) system to combine medication and blood product administration verification with laboratory specimen identification. The wireless system will help track patient prescriptions and dosage.

U.S. Foodservice, a division of one of the world's largest food retailers, awarded Syntegra a contract to survey and implement a new wireless technology environment for the company. Working with Cisco's wireless inventory systems, Syntegra will install devices that will help the U.S. Foodservice distribution center located in Chicago track and monitor inventory.
The initial contract includes a site survey that will be used to measure how many wireless devices will be needed to create the environment. Once the survey is complete, Syntegra will implement the new software.

### 3.4 Service Provider

Every T-Mobile Wi-Fi project has included the full spectrum of activities including; site surveys, design, circuit orders and installations, cabling, network installation, access point and antenna installations, and network management. The T-Mobile teams that are engaged in making each project a success for both T-Mobile and its venue partners are identified and elaborated upon in Section 6.1, Organizational Structure and Staffing Levels.

### 3.5 Relevant Projects

The T-Mobile HotSpot Team has successfully delivered on projects of similar scale and scope as the HiWi project. The following list provides an overview of initiatives with T-Mobile's venue partners.

### 3.5.1 San Francisco International Airport - SFO

Airport Contact: Mr. John Payne, Chief Information Technology Officer
Contact Phone: (650) 821-3375
Address: San Francisco International Airport
P.O. Box 8097
City/State/Zip: San Francisco, CA 94128
Coverage: Public & Private access WLAN infrastructure
Financing Methodology: T-Mobile owned & operated
Project Status: Active
Project Start: January 7, 2003
Phase 1 complete March 28, 2003
Phase 2 & 3 - in progress, est. completion July 30, 2003
Phase 4 - 4Q03
Phase 5 - TBD

Scope: 802.11a and 802.11b WLAN coverage of Terminals 1 & 3, International Terminal and multiple airline clubs (both domestic and international) including United, Delta and American. T-Mobile provided the network architecture design, project management, materials acquisition, staging, installation and cabling of all wireless access points, routers, switches, conduit, cabling and fiber.

### 3.5.2 Dallas-Fort Worth International Airport - DFW

Airport Contact: Mr. William Flowers, Interim CIO/Vice President
Contact Phone: (972) 574-0664
Address: Dallas/Fort Worth International Airport
3200 East Airfield Drive
City/State/Zip: Dallas, TX 75261
Coverage: Public access WLAN infrastructure
Financing Methodology: T-Mobile owned & operated
Project Status: Operational
Project Start: September 2, 2000
Project Completion: March 1, 2001
Scope: 802.11b WLAN coverage of Terminals A, B, C & E, American Airlines AAdmirals Clubs, and the remote car rental facility. T-Mobile provided the network architecture design, project management, materials acquisition, staging, installation and cabling of all wireless access points, routers, switches, conduit, cabling and fiber.

### 3.5.3 T.F. Green (Providence, RI) - PVD

Airport Contact: Mr. David Wilga, Manager of Information Systems
Contact Phone: (401) 737-4000 x240
Address: Rhode Island Airport Corporation
2000 Post Road
City/State/Zip: Warwick, RI 02886-1533
Coverage: Public access WLAN infrastructure
Financing Methodology: T-Mobile owned & operated
Project Status: Operational
Project Start: March 15, 2003
Project Completion: July 24, 2003
Scope: 802.11b WLAN coverage of terminal and gate hold areas. T-Mobile provided the network architecture design, project management, materials acquisition, staging, installation and cabling of all wireless access points, routers, switches, conduit, cabling and fiber.

### 3.5.4 Airlines' Clubs

Although T-Mobile is engaged in 802.11 projects for American Airlines, Delta Airline, and United Airlines, we are providing project information on only two of the Airlines to comply with the project limitation requirements established in the RFP. Should project information be requested with respect to the third Airline, it will be provided upon request.

**3.5.4.1 Delta Airline:**

Airline Contact(s): Tom Fulton
Contact Phone: 404-715-2145
Address: Dept 934
POB 20706
City/State/Zip: Atlanta, GA 30320
Location: Multiple Airports, 42 Airline Clubs
Coverage: Public access WLAN infrastructure
Financing Methodology: T-Mobile owned & operated
Project Status: Active
Project Completion: Target - October, 2003; 16 Clubs currently operational
Scope: 802.11b WLAN coverage within the Airline partner's clubs. T-Mobile provided the network architecture design, project management, materials acquisition, staging, installation and cabling of all wireless access points, routers, switches, conduit, cabling and fiber.

**3.5.4.2 American Airlines:**

Airline Contact(s): Johnathon Bear
Contact Phone: 817-931-4232
Address: 4333 Amon Carter Blvd, MD 5307
City/State/Zip: Forth Worth, TX 76155
Location: Multiple Airports, 33 Airline Clubs
Coverage: Public access WLAN infrastructure
Financing Methodology: T-Mobile owned & operated
Project Status: Active
Project Completion: Target - October, 2003; 24 Clubs currently operational
Scope: 802.11b WLAN coverage within the Airline partner's clubs. T-Mobile provided the network architecture design, project management, materials acquisition, staging, installation and cabling of all wireless access points, routers, switches, conduit, cabling and fiber.

## 4.0 FINANCIAL PROPOSAL

### 4.1 Compensation

T-Mobile will pay to Massport the greater of a Minimum Annual Guarantee or a percent of Gross Revenue. Revenue generated by T-Mobile within those airline clubs and lounges where T-Mobile has an agreement to provide service, will be addressed under separate agreement.

The proposed Minimum Annual Guarantee and percent of revenue shared for providing HiWi in Terminals B, C, D, and the Amelia Earhart Terminal will remain constant should Terminal E be included in the areas to be covered.

#### 4.1.1 Revenue Sharing Percentages

- 10% of net revenue realized on Public Sector service and access including roaming and reselling revenues generated by qualified carrier partners.
- 20% of net revenue realized on all private sector services and access.

#### 4.1.2 Minimum Annual Guarantee (MAG)

Year 1 - MAG - $45,000
Year 2 - MAG - $45,000
Year 3 - MAG - $55,000
Year 4 - MAG - $75,000
Year 5 - MAG - $90,000

Option Year 1 - $100,000
Option Year 2 - $110,000

### 4.1.3 Marketing

T-Mobile expects to spend approximately $275,000 on in-airport advertising at BOS in the first year of the agreement and in excess of $300,000 in each subsequent year.

### 4.2 Data Capture

T-Mobile currently captures the following usage data: Session duration (per minute), megabytes transferred (per megabyte), number of sessions/connections (per user). The capability also exists within T-Mobile back office systems to track and report these metrics per roaming partner in an aggregated summary or individual line item report. Settlement with each partner will then occur either directly with the roaming partner or via an industry standard clearinghouse. Settlement will occur on an agreed upon term between the partners. All data is captured by the use of the radius protocol and network access control mechanisms. T-Mobile's software will require minor modification to support additional roaming partner data capture

### 4.3 Other

T-Mobile believes that sponsorship opportunities will provide yet another means of driving usage and revenue at BOS and, as a result, it will continue to evaluate and participate in most major WiFi industry customer demand generating programs such as Cisco Mobile Office (CIMO partnerships) and other programs sponsored by WiFi mobile device OEM co-marketing and reseller partners as well as other targeted industry influencers. For example, among others this would include computer manufacturers, personal digital assistant manufacturers, computer peripheral manufacturers and handset manufacturers. Other targeted influencers include manufacturers (such as WiFi chipset providers) who sponsor national and international ingredient branding advertising campaigns to drive demand for WiFi services and WiFi enabled mobile devices.

Such sponsorship opportunities are expected to include but are not limited to the following demand generation programs:

- Website marketing opportunities
- Co-branded target advertising
- On-site demonstration events with site partners and national in-direct retailers
- Opportunities to participate in tradeshow exhibits and other events
- Promotions and rebate offers extended directly to customers

## 5.0 Project Schedule

Drawing upon its experience in completing 2700+ WLAN installations, T-Mobile is proposing a project schedule that is both aggressive and attainable. The proposed project plan is based on realistic deployment intervals required to complete key phases of the installation effort, while allowing a reasonable buffer for potential delays. (See Attachment 3 for Project Schedule)

### 5.1 Project Schedule Assumptions

- Massport will assign a project manager to act as an interface and assist T-Mobile with its deployment efforts.
- Permit approvals will be obtained within a reasonable time frame, as defined in the project plan.
- Massport will facilitate badging requirements for installation personnel.
- Use of pre-existing fiber for connectivity between terminals, if required for final architecture / design.
- Asbestos abatement not required

- T1 delivery from the local exchange carrier occurs during standard intervals (30 – 45 business days)

## 6.0 Management & Staffing Plan

### 6.1 Organizational Structure & Staffing Levels

Collectively, the following teams create the T-Mobile HotSpot Team, which will own the design, installation, operations and maintenance of the HiWi project. It is estimated that approximately twelve individuals will form the core team focusing on this project.

#### 6.1.1 Account Management

T-Mobile's Account Management team is focused on the development of the business relationship between T-Mobile and our venue partners. The Account Management team insures the deliverables to our venue partners are met or exceeded and any issues or concerns are resolved in a timely manner.

#### 6.1.2 Program and Project Management

Currently, T-Mobile has two teams focused on the delivery of HotSpot service to our clients' venues. These teams are broken into areas of core focus: 1) Retail project management and 2) Airport / Airline Club project management. This vertical focus enables the project teams to maintain a higher level of knowledge with respect to the venue's operating protocols and procedures, and effectively manage potential issues before they become schedule impacts.

In addition, the Program Management Office provides oversight to the T-Mobile HotSpot program through the coordination of back office initiatives, which support the physical installation efforts driven by the Project Management teams.

#### 6.1.3 Engineering

Partnered with the Program and Project Management teams, the Engineering team provides the network architecture, technical requirements, equipment selection, survey review and overall technical support required to implement WLAN service. The Engineering team also provides technical guidance to field technicians should problems be encountered on site during the course of the deployment effort. In addition, the Engineering team provides final site acceptance for airport venues prior to transitioning a venue to the T-Mobile NOC for operational and maintenance support.

#### 6.1.4 Information Technology

The T-Mobile IT team manages the back office systems required to support authentication to the T-Mobile HotSpot network. This includes the development, implementation and management of custom web pages, billing and authentication support systems.

#### 6.1.5 NOC

T-Mobile's Network Operations Center (NOC) proactively manages and maintains all venues through a variety of network monitoring systems. The T-Mobile NOC manages the resolution of all network, device and circuit outages, as well as any associated cabling issues.

#### 6.1.6 Customer Care

T-Mobile's Customer Care team supports the end user through both voice and email interaction, and takes pride in the level of technology support we can offer to our subscribers. This team is skilled in the support of over one hundred (100) WECA certified 802.11b cards and all major operating systems, including Windows CE hand-held devices (PDA's).

### 6.2 Resumes – Key Personnel

See Attachment 4

## 7.0 OPERATIONS PLAN

### 7.1 Overview

The T-Mobile Hotspot Network Operations Center (NOC), a new state of the art facility located in Carrollton, TX, is staffed with highly skilled analysts and engineers 24x7x365. The facility employs redundant network connections, fail-over hardware, redundant systems, and backup power systems. In addition, the NOC has disaster recovery backup with T-Mobile USA's two operational centers on the east and west coasts.

T-Mobile NOC Staff expertise includes WAN, LAN, WLAN, RF, and general data communications. The NOC staff has certifications that include Microsoft Certified Systems Engineers, Cisco Certified Network Associates, Cisco Certified Network Professionals, and Cisco Certified Network Design Professional. The NOC is structured with network support analysts, team leaders, engineers, manager, and a director.

The T-Mobile NOC has advanced processes and procedures in place that will enable successful support of the Massport HiWi Network. The NOC will monitor all wide area, local area, and wlan devices operating in BOS.

### 7.2 Network Management Systems

The T-Mobile NOC is constantly reviewing new state of the art network, performance, configuration, and security management tools. T-Mobile currently utilizes the following industry standard tools: NetXpert, Remedy, and Metrica. T-Mobile also offers a partner interactive network status website, which will provide Massport with a real-time network status view 24x7. In addition, T-Mobile also has created several customized tools that perform specific functions in regards to WiFi Network Troubleshooting.

NetXpert is an element level SNMP based network management system that conducts proactive polling of all T-Mobile network devices. All devices are loaded into a network database that provides monitoring topology down to the access point level. NetXpert records alarm conditions, and posts alarms to a display that is manned in the NOC 24x7. In the event of a fault condition, NetXpert will receive a Simple Network Management Protocol (SNMP) trap alert from the affected network element. NOC engineers and analysts will acknowledge the alarm condition and follow the appropriate fault resolution process. NetXpert is also used to monitor any ATM backbone based network solution within the T-Mobile network, enabling all alarms to be correlated into one single network management platform.

Metrica is a Web based software application that has been designed to monitor the traffic load on network links. The tool has been customized by T-Mobile Engineering to provide additional performance reporting such as CPU, Buffer utilization and other performance metrics. After each polling interval, the information is immediately posted via java graphical interface to an internal web interface solution for viewing. In addition, the tool has also been customized to produce a Top 10 report of the busiest interfaces for each 24-hour period. This application allows the NOC and engineering to perform near real time load analysis along with long-term capacity planning activities.

### 7.3 Trouble Tracking and Issue Resolution Process

All issues are tracked by the use of the Remedy trouble tracking system. Each ticket remains open until problem resolution has occurred. Upon discovery of a network outage or service impacting issue, a NOC engineer will immediately open a trouble ticket, using the following severity guideline

- ***Severity 1 Critical Impact:*** Multiple Access Zones down at BOS or total airport coverage is down; problem causes a critical impact to business functions of multiple BOS Access Zones or customers. Immediate response is required.

- ***Severity 2 High Impact:*** Single Access Zone down or service degradation of multiple Access Zones; problem causes a critical impact to business function(s) or customer(s). Immediate response is required.
- ***Severity 3 Medium Impact***: Service degradation of a single Access Zone; problem causes a critical degradation of service, resulting in a medium impact to a single Access Zone, business function, or customer.
- ***Severity 4 Low Impact:*** All requests and problems that can wait for a fix; problem causes a low impact to business function(s) or customer(s). A workaround is provided. Includes scheduled maintenance.

The NOC follows detailed procedures to ensure that the fault resolution process is being followed properly. The NOC staff maintains both soft and hard copies of all procedures. Procedures are saved on a shared limited access drive, and are backed up on a nightly basis.

In most cases, T-Mobile NOC engineers take ownership and manage the repair of all other vendor and partner network issues. All issues are tracked in the Remedy Ticket System, as per the severity level of the issue. NOC engineers coordinate problem resolution as required, utilizing all available resources. Problem escalation occurs per vendor, partner, and T-Mobile escalation procedures. Notification occurs per agreed upon customized procedures.

The T-Mobile Hotspot NOC engineers will utilize all available documentation and exhaust all means necessary to resolve each issue at their level. If unable to resolve the issue at their level, the NOC engineer will escalate the problem per the Network Operations Escalation Procedures.

The NOC is the primary interface to support new Access Zone integration. NOC engineers validate that each circuit has been installed and tested, and that equipment installations are accomplished per T-Mobile standards. This also includes equipment configuration verifications and security management. In addition, the NOC staff verifies that the proper documentation has been provided to manage the site. NOC engineers provide second level support for any technical issues involved with new site activation that the vendor cannot resolve. New sites are loaded in the NOC NMS databases as they are integrated into the network.

### 7.4 Moves, Adds, and Changes

NOC engineers coordinate all moves, add and changes to Access Zones. Each airport operational modification follows a formal change management process, and is scheduled according to business justification. All asset changes are noted, and entered into the documentation tracking process. NOC engineers verify that all modifications to existing sites are loaded into the NOC NMS. All assets are tracked and catalogued via project management and inventory systems. Communication of MAC activities will be made to Massport per the established lease agreement for all scheduled maintenance.

### 7.5 Network Reliability, Reporting and Notifications

The T-Mobile Network Operations Team will produce network availability metrics to T-Mobile Management and Massport on a monthly basis. Real-time network status reports will be made available via the Massport via the partner interactive website.

The Network Operations Center performs real-time outage reporting via a web interface 24x7. The web page is directly integrated with the Remedy trouble tracking system and depicts a summary of all service-impacting issues. The partner page is accessible through a secured SSL login that requires a specific user ID and password. The outage summary contains the following information: Site ID, NOC ticket number, date, outage time period, description of problem, estimation of customer impact, and resolution details. In addition to the current outages web page, a recent service interruption page will be made available for Massport to view past customer affecting events.

In the event of a major service interruption, the NOC sends out notification emails and pages per pre-determined operational procedures. PAWLAN Partners as notified of service interruptions per pre-established lease agreement commitments.

The NOC staff notifies the T-Mobile technical organization as soon as possible in the event of any severity one issue. Technical escalation occurs as per the Network Operations Center escalation procedure, and the NOC staff sends out an email notification to a Customer Service and Sales distribution list for all severity one issues. (See Attachment 5 – NOC Reports)

### 7.6 Scheduled Maintenance

The Hotspot NOC utilizes Change Management processes that allow proactive notification of all scheduled maintenance that has potential to impact subscriber service. All Change activities are managed through the Remedy trouble tracking system. Notifications will be made to Massport per the agreed upon lease agreement with a minimum of 48 hours prior notice before the maintenance activity is scheduled. Emergency maintenance that must be performed immediately will be treated as a normal service interruption, and notification will occur as required.

### 7.7 Field Service

T- Mobile has subcontracted with several nationwide field maintenance providers to provide on-site service and maintenance. T-Mobile will provide support 24 hours a day, responding in 4 hours or less.

The Hotspot NOC coordinates all field service maintenance activities for the Massport HiWi Network. Current field maintenance partners include Vital Network Services and Cisco Systems. Vital Network Services provides onsite troubleshooting support for radio frequency and cabling issues. T-Mobile maintains a 4-hour onsite response time agreement with Vital.

Cisco provides 24x7x4 SmartNet Premium Service for Massport. Cisco's agreement includes onsite maintenance support, RMA parts replacement, software upgrades, and phone support.

### 7.8 Customer Care

The philosophy that drives the T-Mobile's customer service program is the belief that the level of customer care delivered should both consistently exceed the expectation level of those we service and be uniformly delivered regardless of the medium used in providing the service. To ensure that the premier customer care standards are met and maintained, the employees of T-Mobile HotSpot Customer Service are required to possess the highest level of expertise in 802.11 technologies.

Accordingly, support personnel are trained on over 100 WECA certified 802.11b PCMCIA cards, all major computer operating systems and Windows CE handheld devices (PDAs), as they relate to connectivity to the T-Mobile HotSpot network.

Delivery of customer care services includes real-time technical and billing support which are managed both by Email and telephone. Skills-based routing is utilized to ensure that each contact is handled appropriately and expeditiously. Customer Service can be reached via telephone or via email. Self-help customer service is also publicly available on the Internet website.

Refunds and credits are handled on an individual basis and each request is judged on its own merits. The Customer Service Center has personnel available to review account information with customers and address any billing concerns presented. Each customer has the right to escalate their request, as they deem appropriate.

T-Mobile HotSpot Customer Service fields thousands of help requests each month.
The Tier I group within the T-Mobile HotSpot Customer Service Center handles general questions about the service and Billing questions. Technical assistance is handled by highly trained Technical Support Specialists in the Tier II group.

Non-native English speakers communicate with T-Mobile HotSpot primarily in English. When the need arises, non-native English speakers are available within the Customer Service Center to provide the necessary support. (See Attachment 6 – Customer Care Reports)

## 8.0 TECHNICAL PROPOSAL

### 8.1 Overview (a)

The proposed HiWi solution is comprised of three parts:

- The access network
- The public and private vendor specific network
- T-Mobile's back-end network

The access network is a common network that is shared by both public WLAN service providers and private applications. It is made up of Access Points (AP), access switches, distribution switches, core switches and connecting CAT-5 UTP and fiber. Optionally, this access network can be transported through an existing Ethernet network.

The public and private vendor networks depend on application, but typically are made up of routers, connections to either the Internet and/or a private network and optionally network gateways and servers. Each WSP, vendor, or private tenant will be required to add its own supporting equipment. In T-Mobile's case, this portion consists of a router or routers and T1's to T-Mobile's back end.

T-Mobile's back end has, Points of Presence (POP), Network Operation Centers (NOC), an ATM and data network, routers, gateways, Radius servers, web page servers, and firewalls. Network management of the access network and T-mobile's router is done from the NOC. Other WSPs will be required to manage their own network portion.

The proposed solution has the following features:

- Provides 802.11b and 802.11a data network services.
- Provides a Neutral Host / Open Access / Equal Access platform that allows multiple Wireless Service Providers (WSP).
- Provides the capabilities to expand the network to accommodate overlays of emerging wireless technologies whether licensed or unlicensed.
- Capable of sustaining high levels of Quality of Service.
- Network security features – Authenticates users and limits hacking and network abuse.
- Coverage within the designated portions of Terminals B, C, D, Amelia Earhart Terminal and optionally Terminal E.
- Private-side application support – The airport can share the HiWi network's Access Points for applications such as Mobile Ticketing, Baggage Reconciliation, Wireless FIDS, Wireless CUSS, Remote Cameras, Wireless Magnetometers, Wireless Point of Sale terminals, and E-mail.
- Subscriber Access Control – Subscribers are authenticated before being allowed access to the network.
- Subscriber Roaming – Allows subscribers of another WSP to gain access permission to use this network.

- Subscriber Mobility – Subscribers can switch access points throughout the covered areas without loss of connection. Sometimes referred-to as a hand-off.
- Billing – Subscribers are billed for their usage. Customers may receive combined billing with their PCS telephone bill if they are T-Mobile PCS users.
- Location-Based Services – Subscribers can see a different log on page depending on the location where service is initiated.
- Unrestricted Internet access.
- E-Mail forwarding – Enables a subscriber to send e-mail from a proxy. The subscriber can send e-mail without reconfiguring their e-mail client.
- VPN support – Allows subscribers to securely tunnel through to their home network.
- 24 Hour Technical Support Hotline and customer service support.
- 24x7x365- Fully manned redundant Network Operations Centers.

### 8.1.1 Quality Assurance Plan

T-Mobile has successfully deployed the HotSpot network in multiple airports throughout the US, for both airport-wide and airline club coverage. As a result of these deployment efforts, T-Mobile has established a set of standards by which our installation teams operate within the airport environment:

- All field personnel trained and adhere to both T-Mobile and our venue partner's Code of Conduct, OSHA guidelines and venue specific operational guidelines including badge access / escort requirements, maintenance windows and safety procedures.
- As part of the joint development of the installation project plan, we will work with the point of contact from the venue partner to ensure major activities at the location are not in conflict with other facility improvement programs, thus mitigating operating impacts.
- Work is typically completed "off-hours" so as to minimize disruptions to passengers.
- Existing facilites (cable tray, conduit, etc.) are used where possible to decrease new infrastructure installation.
- Weekly status meetings are conducted with our venue partners as both a status and issue identification forum.
- All equipment is installed in compliance with manufacturer specifications and any local, state or national codes, including N.E.C. and IEEE.

### 8.1.2 Facilities and Utilities

Public and private access will require rack space at the Main Distribution Frame (MDF) location. Gateway, switches, routers and servers will be placed in these racks. The MDF will need to be close to or co-located with the MPOE and/or T1 NIUs. This location must provide the capacity to cross connect the Gig-E network to the airport LAN and all airline LANS as well as connections to the public Internet or private networks. Connection to the airlines' LANs may require additional networking to reach their network access points. Proper placement of the MDF(s) will assist further installation phases and provide immediate public and private access that will provide the necessary spatial redundancy. An MDF typically has one or two six foot 19" racks to hold switches and routers, UPSs, power conditioning, and cable management.

Cisco 3350-12G distribution switches will be located in Intermediate Distribution Frames (IDFs) as needed. Distribution switches require 100 to 127 or 200 to 240 VAC (auto-ranging), 50 to 60 Hz, 65W (maximum). Access switches need an environment that is between 32 and 113° F (0 to 45° C) and a relative humidity of 10 to 85% (noncondensing). Access switches produce 222 BTUs per hour maximum. An IDF will typically have one or two distribution switches in a two foot 19" rack. Cable managers are used to control excess fiber. Fiber from IDFs to LDFs and MDFs is typically run in existing conduit. New conduit will be installed if required. Additionally, Local Distribution Frames (LDFs) will be required for access switches. Typically a Cisco 3550-24-PWR is used for access switches. Power will be required at each LDF to power the distribution switch and up to six access points.

Access switches require 100 to 127 or 200 to 240 VAC (auto-ranging), 50 to 60 Hz, 65W (maximum). Access switches need an environment that is between 32 and 113° F (0 to 45° C) and a relative humidity of 10 to 85% (noncondensing). Access switches produce 222 BTUs per hour maximum. An LDF will typically have one access switch, a patch panel, a power conditioner, and cable management.

Access points are powered by the access switch using Power over Ethernet. The access points are plenum rated and can tolerate an environment that is between minus 4° to 122°F (-20° to 50°C) and 10 to 90% humidity (noncondensing). Each access point will draw up to 11 watts of power. An LDF will typically support between 3 and 6 APs. CAT-5 UTP is typically run in conduit or interduct to the APs where required.

T-Mobile will require secure storage for spares near or in the MDF. Access should be limited to Massport Authorities, certain T-Mobile employees and service contractors thereof.

### 8.1.3 Y2K Compliance

All HiWi equipment is Y2K compliant and will be certified as such prior to commencement of operations.

### 8.1.4 Intermodulation Study

T-Mobile, if selected, will provide an intermodulation study relating to the appropriate operating frequencies within the 2.4 and 5 GHz bands prior to access point installation.

## 8.2 Radio Frequency Survey (b)

T-Mobile has implemented a stringent survey methodology to ensure the quality of the WLA footprint, and subsequent quality of the network installed. All survey technicians are required to follow pre-established guidelines and operating procedures specific to the environment in which they are working. Included in these guidelines are OSHA requirements, venue Code of Conduct, access and technology requirements.

RF Surveys are broken into three (3) major areas of activities:

- Access Point placement and interference detection
- Cabling / fiber paths (including intermediary cabling closets and any equipment space requirements)
- Primary equipment placement (routers, T1's, equipment rack, power requirements)

### 8.2.1 Access Point Placement and Interference Detection

During the course of determining Access Point placement, survey technicians will place access points in various locations throughout the intended coverage area to identify the preferred placement for coverage. Upon identification of the preferred placement, the technician will take a digital photograph of the intended AP placement as well as marking the intended location on a floor plan of the facility. Channel identification, power output, antenna location / orientation / attenuation, SNR readings, and any encountered interference will also be identified and documented at this time.

### 8.2.2 Cabling / Fiber Paths

In conjunction with the Access Point placement, the survey technicians will be identifying viable cabling paths to reach the intended Access Point location. Technicians will determine these paths based upon IEEE cabling standards for LAN cabling, venue requirements for cable tray, conduit, and any asbestos requirements in addition to any unique requirements for local, state and/or national code. Intermediary closets will be identified for equipment placement as an aggregation point to the various access points proposed for the airport. All cabling paths will be identified on floor plans, showing the proposed path from the Access Points to the intermediary cabling closet, riser or closet-to-closet cabling requirements, and cabling requirements back to the primary equipment location.

### 8.2.3 Primary Equipment Placement

Placement of the primary equipment (routers, T1's, etc.) to support the WLAN deployment is typically in a central airport controlled telecommunications room. T-Mobile, in conjunction with Massport, will identify any existing racks that may be utilized for placement of the primary equipment. If existing racks are not available for use, proposed locations will be identified for new equipment racks to be installed. Power requirements will be determined in conjunction with the identification of the proposed primary equipment location. All proposed rack locations will be identified and documented on venue floor plans.

In addition, general information will be collected specific to the intended coverage areas, which impact the proposed equipment placement:

- Atrium / glass enclosed areas
- Raised / solid ceilings
- Structural constraints
- Unique site access information / constraints not previously identified

### 8.2.4 Survey Documentation

All collected information will be consolidated into a single Site Survey document providing a comprehensive overview of the physical and logical connectivity requirements. T-Mobile's Network Engineering team will subsequently review the Site Survey document and finalize the site-specific network architecture.

Upon completion of RF Survey and Engineering architecture, T-Mobile will provide Massport a document which will identify proposed equipment, specifications and placement, cabling paths, power requirements, RF propagation, channel assignment, and any additional documentation relevant to the installation effort.

## 8.3 Network (c)

### 8.3.1 Network Design

The proposed HiWi network is comprised of Access Points connected to Access Switches. These access switches are connected in turn to Aggregation Switches. The aggregation switches are in turn connected to core switches. Both private and public equipment such as routers, gateways and servers connect to the core switches. (See Attachment 7 - T-Mobile Generic Architecture)

Access Points (AP) are Cisco 1200s, running both 802.11b and 802.11a. The access points are powered using Power Over Ethernet. APs connect into access switch locations throughout the airport with CAT-5 cable not to exceed 328 feet. The access switches in turn connect to a Gig-E Fiber network comprised of single mode or multi-mode fiber, depending on the distance between nodes.

To access the T-Mobile network, subscribers can use laptops, PDAs, tablets or other devices using the 802.11 protocol. T-Mobile's network is operating system agnostic. This means the subscriber can run Windows, Apple OS, Linux or other operating system. The network provides subscriber mobility through mechanisms available in IEEE 802.11 standards. This provides the ability for subscribers to freely roam from one access point to another. No additional client software is required.

Access Points are deployed using unlicensed ISM frequencies in the 2.4GHz to 2.4835 GHz band. The frequencies in the 2.4GHz band are re-used in a 3:1 reuse pattern using channels 1, 6 and 11 (2412, 2437, and 2462 MHz). Typical power output on the 2.4 Ghz band are between 20 and 100 milliwatts. 802.11a operates in the U-NII 1 and U-NII 2 band (5.150 GHz – 5.350 GHz). The frequencies in the 5.1 and 5.2 GHz band are re-used in a 7:1 re-use pattern using channels 36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz). One channel is used as a spare for fill-in. Typical

power output on the 5.1 and 5.2 GHz band is between 20 and 40 milliwatts. The 5 GHz cells will overlay the 2.4 GHz cells.

Maximum data transfer speeds for 802.11b is 11Mbps while 802.11a is 54 Mbps. Though the over-the-air transfer speed of 11Mbps and 18Mbps is typical, the actual throughput is limited by the throughput capacity of the backhaul. In the case of this deployment T-Mobile would propose there be two (2) T1s, or 3 Mbps maximum. Since the T1s are shared with all users in the wireless network, the nominal throughput should be at a minimum 200 Kbps as observed by an individual user. As more capacity is required, additional T1s will be added to the network.

It is expected that one or more SSIDs will be used per tenant on the network. The network supports a maximum of 15 SSIDs per access point. Of this number, T-Mobile expects to reserve two SSIDs for its purposes. The rest of the SSIDs are made available for public and private applications. Each SSID maps at the access point to a secure VLAN that carries the data to either the public or private interface of the system. The APs support 16 secure VLANs, one of which is reserved for management purposes to fully separate user traffic from management traffic.

The proposed HiWi network supports multiple Wireless Service Providers (WSPs) directly as well as through traditional roaming. Public access for other WSPs is routed to the T-Mobile or WSP tenant's equipment, router(s) and appropriate Internet facilities. Traffic is authenticated by each WSP. T-mobile serves up location-based customized splash pages, authenticates and bills its users, handles roaming authentication and manages the network remotely from either of two Network Operation Centers (NOC). Also, the NOC can host custom applications or services. Other WSPs may choose to do the same or use a capture portal / zone controller co-located at the airport.

Private access of the system passes through the gateway to a private switch, connected to the airport's and airlines' LANS. Private access passes through completely separate secure VLANs, separating public from public access. A private Access Gateway or Bridge can provide additional layers of security and control for the private access.

### 8.3.2 Redundancy

Redundancy is built into the HiWi network at the core where failure of a link or component can mean a total outage. T-Mobiles network to meet the required service levels. Measures to maintain high reliability are included in the network design to support airlines' and tenants' critical operations. The exact design of the network depends on the physical location of MDFs and their network interconnection. (See Attachment 8 - Redundancy in Preliminary Architecture)

### 8.3.3 Security

T-Mobile and Cisco have worked together to develop security features for the Public Wireless LAN market for both routers and switches. T-Mobile uses a combination of enhanced ACLs, sound switching and routing rules, and stateful firewalls to limit hacking and network abuse.

The router local to the venue employs Authorized ARP. The router will only route IP traffic for subscribers that have a current ARP table entry. Address spoofing is restricted using Unicast Reverse Path Forwarding (RFP). Packets without a verifiable IP source address are discarded. Denial of service attacks are throttled by rate limiting.

Management is on a separate VLAN from subscriber data and given adequate bandwidth through QoS measures. Inter-client communication is limited with Publicly Secure Packet Forwarding (PSPF) and Private VLAN / Port Protection. Traffic cannot be forwarded between protected ports at Layer 2, but rather all traffic passing between protected ports must be forwarded through a router. ACLs limit source and destination addresses.

The T-Mobile backbone makes two tier-1 connections to the Internet through one of several border routers and stateful firewalls. T-Mobile subscribers are assigned a private IP address that is NATted to the Internet.

### 8.3.4 Standards

The networks installed by T-Mobile meet applicable standards such as IEEE 802.11b, 802.11a, 802.3, 802.1d, 802.1q, 802.1p, and 802.1x, and IETF RFCs.

## 8.4 Usage Monitoring & Reporting (d)

T-Mobile currently captures the following usage data at each of its HotSpot locations: Session duration (per minute), megabytes transferred (per megabyte), number of sessions/connections (per user). The capability also exists within T-Mobile back office systems to track and report these metrics per roaming partner in an aggregated summary or individual line item report. Settlement with each partner will then occur either directly with the roaming partner or via an industry standard clearinghouse. Settlement will occur on an agreed upon term between the partners. All data is captured by the use of the radius protocol and network access control mechanisms. T-Mobile's software will require minor modification to support additional roaming partner data capture. (See Attachment 9 User Experience Screens; Attachment 10 Usage Reports)

## 8.5 Access Control (e)

The T-Mobile backbone makes two tier-1 connections to the Internet through one of several border routers and stateful firewalls. T-Mobile subscribers are assigned a private IP address that is NATted to the Internet.

### 8.5.1 Standards

The networks installed by T-Mobile meet applicable standards such as IEEE 802.11b, 802.11a, 802.3, 802.1d, 802.1q, 802.1p, and 802.1x, and IETF RFCs.

The user enters user name, password and submits. When the subscriber is authenticated and authorized, a logoff pop-up window is presented for the Internet service and a T-Mobile Wireless Broadband welcome page is launched in a separate window.

User now has Internet connectivity and can browse the web, e-mail, open a VPN tunnel to their home office, or use other Internet services such as chat. If an error occurs during the logon process, an error pop-up window is displayed.

### 8.5.2 Roaming Access

A roaming subscriber will view a link pertaining to their WSP or roaming service on the initial log-in page. The subscriber will click on that link, bringing up a new login page for the roaming WSP. The appropriate log-in credentials are passed from T-Mobile's Radius server to the roaming partner's Radius server where they are authenticated. Upon receiving the response from the roaming Radius server, the roaming subscriber will receive the roaming network's welcome page and the small log-off window.

### 8.5.3 Open Access Tenant Access

An open access tenant subscriber's device associates with an access point using the appropriate network's SSID. The user's device then initiates a DHCP request, which is routed to the tenant's router over the VLAN associated with the tenant's SSID. When the subscriber opens a web browser the web page request is forwarded to the tenant's network and processed just as it is processed over their native network. With this access control mechanism, the subscriber is not aware of the presence of any other network besides the native network. The login procedure is identical to the one to which the customer is accustomed.

### 8.5.4 Private Access

A private user's device associates with an access point using the appropriate network's SSID. When the user's device initiates a DHCP request, it is routed to the private network's router over the VLAN associated with the private network's SSID. Alternatively, the private user's device can have a fixed IP address. Subsequent transactions are sent through the router to an access controller, which can further authenticate the access.

## 8.6 System Expansion Capability (f)

Please refer to section 8.7.1.1

## 8.7 Detailed Technical Requirements (g)

### 8.7.1 Technical Requirements

#### 8.7.1.1 System Expandability

##### 8.7.1.1.1 Expandability-Capacity

The capacity of the backhaul is the limiting factor in this network. As coverage is added and greater numbers of subscribers are supported, additional T1 backhaul capacity will be required. It is expected that two T1s will be initially required for use by T-Mobile. With increased use of the system by subscribers and tenants, additional T1 backhaul may be required. In this way, access to the public Internet is protected from erosion by public access users.

Reliability statistics will be monitored. If there is an indication that an upgrade is necessary to improve the reliability of the system, a determination will be made as to hardware and/or software upgrades required.

##### 8.7.1.1.2 Expandability-New Network Components

The network design will be provisioned with gigabit Ethernet between MDF, IDF and LDF switches, this will provide sufficient capacity to handle increased usage from public, Airline/Tenants and Massport users for the foreseeable future. If additional capacity, switches and Access Points are required, MDF, IDF and LDF switches will have a built in 20% spare port policy to accommodate such needs.

The actual limiting factor in this network will be the T1 backhaul capacity. As coverage is added and greater numbers of subscribers are supported, the addition of an additional T1 may be required. It is expected that one T1 per terminal will be initially required.

##### 8.7.1.1.3 Expandability-Emerging Technologies

It is not expected at this time that 802.15 (Bluetooth) will become a widely developed standard for wireless networking. It is possible that the Infrared version of 802.15 may become commercially viable. In that case, T-Mobile will either deploy such a service or engage with another service provider for deployment.

The network will initially be deployed to support 802.11b and 802.11a to cover the 2.4 and 5.2 Ghz bands.

The Access points may need a software upgrade to support WPA to improve security. This upgrade will be dependent upon when the standard becomes available and when the software upgrades are made available from the vendors.

802.11i may eventually be deployed to improve security. This is expected to be a software upgrade. Acceleration upgrades may be required in all access points to support AES encryption. This upgrade is forecast in 3Q2004 at the earliest and will take approximately two to three weeks to complete.

The network will be updated at no cost to the Airport to support new technologies when the following are satisfied:

- The product or software meets T-Mobile's manageability requirements
- The product or software meet both T-Mobile's and security requirements
- The product or software enhancement is commercially viable and has a valid business case
- A suitable vendor makes the product or software
- The product or software meets T-Mobile's testing and quality requirements

#### 8.7.1.2 System Integration into the Airport Network

T-Mobile can integrate HiWi into Massport's data network. However, our experience with other venues has indicated that it is beneficial for security reasons to physically separate unsecured traffic from secured traffic, especially in critical networks such as those that are present at airports. If an integrated network is desired, it is highly recommended that Massport and T-Mobile develop and implement a strong mutual security policy.

It should be noted that this system integration is not our preferred method due to security, billing, manageability and quality of service issues. Due to the nature of a public wireless LAN, we do not permit client-to-client communication without first going through a router. Not doing so would mean that we could not bill for or limit resource intensive uses such as file sharing and gaming. Before using Massport's data network, we would need specific security policies to be in effect which may not be compatible with typical operations in an airport. Also, system integration may impair our ability to respond to network outages or capacity issues since we won't have visibility into Massport's data network.

A more preferable suggestion is physically separating the HiWi network from Massport's data network and providing a secure access gateway or bridge between the two networks. Only properly authenticated users based on Massport's own security policies, should have access to Massport's secure data network through an access gateway or bridge.

#### 8.7.1.3 Operational Requirements

##### 8.7.1.3.1 Compliance

The T-Mobile system is fully compliant under the applicable sections of 47 CFR part 15.247 Direct Sequence Spread Spectrum Systems, 47 CFR parts 15.401, 15.403, 14.405, and 15.407 Unlicensed National Information Infrastructure Devices.

The use of wireless devices on an aircraft with the door closed, whether it is sitting at the gate, taxiing, or in flight, while prohibited by the FAA and other Civil Aviation Agencies worldwide, is not within our control. However, T-Mobile has no intent to provide public access wireless LAN to serve passengers while on board an airplane. T-Mobile will work with airlines to provide operational support. Some Carriers may utilize 802.11b on aircraft while "door open" at a gate. T-Mobile will assist airlines in passing their information across the HiWi network and onwards to their respective LANs.

The networks installed by T-Mobile meet applicable standards such as IEEE 802.11b, 802.11a, 802.3, 802.1d, 802.1q, 802.1p, and 802.1x, and IETF RFCs.

The HiWi network will be extended to provide an 802.15 (Bluetooth) compliant service when the market for this service develops.

The HiWi network will be compliant with 802.16 (Wireless Metropolitan Area Networks) when this service is required to link locations wirelessly to other locations, such as connecting the main terminal to remote buildings.

#### 8.7.1.3.2 Seamless Coverage

The network will provide reliable, seamless network coverage. AP-to-AP roaming will be enabled on the system. The system will also provide subnet roaming.

#### 8.7.1.3.3 Capacity

The network will have the capability to add capacity and support new technologies as markets develop.

#### 8.7.1.3.4 FHSS & DSS

The network will fall back to a lower data-rate when the signal levels are inadequate. The fallback can be due to out of range situations and interference.

On 802.11b the supported data rates are: 1, 2, 5.5, and 11 Mbps. On 802.11a the supported data rates are: 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

If and when market opportunities present themselves for other services, we may choose to deploy them as long as they do not interfere with the 802.11b and 802.11a service. T-Mobile will make every effort to satisfy the wireless needs of all public and private users of the system. If use of another standard is required, T-Mobile will consider the implementation of other standards such that they do not interfere with existing systems.

#### 8.7.1.3.5 Channel Assignments

The network will use channels 1, 6, and 11 (2412, 2437, and 2462 MHz) in a 3:1 channel re-use for the 802.11b deployment. Channels 36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz) will be used with a 7:1 channel re-use pattern with a spare channel to support 802.11a. The site survey will determine the use of frequencies.

Roaming will occur through the VLAN connections on the network side. Channel assignments will not affect roaming on the system.

#### 8.7.1.3.6 Transmitter Power Output

Transmitter power will be limited to 100mW max on 2.4GHz and 40mW max on 5 GHz. Access Points are typically run at 20 mW power out on 2.4Ghz and at 40mW on 5 GHz so that the cell will provide similar coverage on both bands. In some cases, power will be set at different levels to either extend or increase coverage.

#### 8.7.1.3.7 Integration with Airport-Wide Wireless Lan System

Private access on the WLAN system will be provided without requiring specialized installation on the client device. The airport LAN, various airline LANS, and other networks will connect to the WLAN network through the private access components via CAT-5 Ethernet connections. A connection between the client device and their network will be established through clientless authentication. Once authenticated, the private access system will facilitate the customer implementing additional security depending on the desires of the customer. Additional security is available through the implementation of a client application, but this is an option and not required for standard system use.

Access to any unsecured, public portion of the network can be clientless. Operation may require an 802.11b/a/g card and associated drivers. Such access will provide user authentication, but not user data confidentiality, data integrity and non-repudiation. Subscriber data to and from a clientless subscriber must be secured using https:, SSL, SSL tunneled E-mail, etc.

However, access to any secured portion of the network will require specialized software, drivers and/or equipment in order to provide authentication, data confidentiality, data integrity and optionally non-repudiation. T-Mobile's public wireless LAN application may require secured access and thus client software.

**8.7.1.3.8 Collection of System Usage Data**

T-Mobile will report usage data that includes it own subscriber traffic and roaming traffic to Massport. Other public or private tenant WSPs will report their traffic in a similar manner. T-Mobile will also monitor circuit utilization and traffic via SNMP collection and other methods. This information could be used to help validate and verify the usage information provided by public and private tenant WSPs. Additional information may be collected and reported based on specific needs of Massport, public and private tenants.

**8.7.1.3.9 Operating, Maintaining, and Upgrading**

T-Mobile will be solely responsible for operating, maintaining, and upgrading the wireless network to provide service and continuously enable access to the deployed technologies. As new wireless technologies emerge, the network will be updated at no cost to the Airport to support new technologies when the following are satisfied:

- The product or software meets T-Mobile's manageability requirements
- The product or software meet both T-Mobile's and Massport's security requirements
- The product or software enhancement is commercially viable and has a valid business case
- A suitable vendor makes the product or software
- The product or software meets T-Mobile's testing and quality requirements
- T-Mobile will make a proposal for upgrade to Massport once a new wireless technology meets these requirements

**8.7.1.4 Interoperability**

The networks installed by T-Mobile meet applicable standards such as IEEE 802.11b, IEEE 802.11a, and IEEE 802.3. This equipment is certified to be interoperable by the Wi-Fi Alliance. The network will be interoperable with Wi-Fi approved wireless network cards.

**8.7.1.5 Site Survey**

**See 8.2 through 8.2.4**

**8.7.1.6 Coverage Areas**

T-Mobile network design will cover public access areas in terminals B, C, D, the Amelia Earhart terminal, and optionally terminal E, outside of security such as ticketing, baggage claim, common areas, and public areas behind security such as concourses, gate areas, airline clubs, restaurants, and airport private areas such as baggage handling. Outdoor coverage will be provided in the ramp areas around terminals B, C, & D and optionally E (and not by the Amelia Earhart Terminal), and will be covered to at a minimum of 50 feet past the end the airplane. (See potential conflict in RFP requirements between Section II, Paragraph 1 and Appendix D section F, Paragraph 1.)

When additional coverage is needed in the future T-Mobile network design will be able to accommodate additional capacity, switches and Access Points as needed. Since, MDF, IDF, and LDF switches have a built in 20% spare port policy for further network expansion.

**8.7.1.7 Location of Access Points**

Our deployment is such that access point coverage areas overlap such that two or more access points can be reached from most points in the coverage area. Our coverage area is defined by a minimum signal to

noise ratio of 15dB. The actual location of access points will be determined during the site survey process.

#### 8.7.1.8 Load Balancing

Client cards that are in areas of overlapping coverage will normally associate with the strongest signal and not with the lightest loaded access point. Load balancing is supported by the Cisco 1200 access points, which provide information on number of users, bit error rates, and signal strength to client devices. However, an accompanying client card such as a Cisco 350 must be able to read this information in order for it to select the Access Point that provides the best network connection.

#### 8..7.1.9 RF Interference

Use of the 2.4 and 5.2 GHz bands is regulated under part 15 of the FCC's rules. These rules dictate that there are no guarantees to interference-free communications, and only offers protection from harmful interference. As such, interference will be mediated and/or resolved first between the involved parties and T-Mobile. If no common ground or solution to the problem can be found, a neutral RF consultant may be hired at the cost of the involved parties to resolve the issue(s). The FCC is currently considering adding more frequencies to WLAN (500MHz and 3.7GHz under part 15 or a new part yet to be determined. It is recommended that Massport enforce a wireless policy that restricts placement of devices in said frequencies.

#### 8.7.1.10 Network Security

##### 8.7.1.10.1 Public WLAN

Our solution for T-Mobile's Public access network will have two levels of security:

- Our clientless service allows easy sign-up but does not provide data confidentiality. This service authenticates subscribers and depends on secure services such as https, SSL and VPN to provide data confidentiality. All log-on, account and/or credit card information is secured using SSL. This is currently implemented.
- Our more secure service uses 802.1X for port based network access control. The authentication protocol is one of several EAP types. Subscriber data will be encrypted for data confidentiality. This technology is currently in the development phase and should be deployed during 2004.

Encryption remedies packet snooping / interception attacks as authentication cannot. However, authentication can solve the problem of fabrication attacks (false data).

Security for the WSPs access will be the sole responsibility of the WSPs.

##### 8.7.1.10.2 Private WLAN

In order to better secure the communication of traffic on the private WLAN, the system provides authentication through a web-based system using SSL. Browser-based authentication requires a user to enter authentication information on a login Web page before being able to access other resources on the network. The network management system detects the user attempting to access the network; it displays the login page and allows the user further access only if the user provides valid authentication credentials (typically, a user name and password).

This approach provides wide compatibility with user systems and equipment. It is important to note that the SSL connection is for authentication only. Further security is necessary to encrypt wireless data.

When an authorized user attempts to access the network, the Vernier Networks System adjusts the network configuration to support the user's device, without requiring any custom software or

reconfiguration of the user's device. The system integrates with whatever authentication systems the private access user already has in place, such as RADIUS, LDAP, or Kerberos.

To protect network traffic from eavesdropping and tampering, the system supports a broad range of encryption technologies, including:

- 802.1x
- IPsec (the encryption technology commonly used by VPNs)
- L2TP (Layer 2 Tunneling Protocol)
- PPTP (Point-to-Point Tunneling Protocol)
- IPSEC-3DES
- AES (Advanced Encryption Standard)

Each Access Manager blocks unauthorized users from the network, enforces access policies for authorized users, and functions as an IPsec termination point. By offering local termination compatible with the leading VPN clients, the Vernier Network System enables network administrators to leverage their investment in VPN clients to secure their wireless networks, while offloading traffic from already overburdened VPN concentrators. The system uses VPN technology to secure the airwaves, without compromising VPN performance.

802.1x has been shown to have flaws enabling session hijacking and man-in-the-middle attacks. The attack is usually accomplished by changing the sequence numbering of a packet. The proposed private system has inherent protocol designed to protect it from hijacking and man-in-the-middle attacks.

The problem with 802.1X is that supplicants currently only exist for Windows XP and Windows 2000. Products like Windows 98, ME, NT4, Linux/ FreeBSD / OpenBSD and Apple 9 and X are unsupported. Wi-Fi Alliance's WPA, which includes SSN which provides TKIP data protection and the 802.11i which includes WPA and AES-based data protection are still in the planning stages. Since our service uses only infrastructure, Peer-to-peer or ad-hoc services like iBSS are not supported by our network. As a result, the Ad hoc mode protection feature of 802.11i will likely not be implemented.

#### 8.7.1.11 Vendor Specific Solutions

We intend on using Cisco 1200 access points, which are capable of 16 VLANs and 15 SSIDs. Symbol makes an access point, which is capable of only 4 SSIDs.

We intend on using Cisco 3550-24-PWR and 3550-12G switches, 1721 and 3745 routers that utilize security features co-developed by Cisco and T-Mobile.

#### 8.7.1.12 System Performance

Our network can provide reports to the airport that include number of users on the WLAN, the total usage time, the number of customer complaints, the time the network was available and any outage times. Also, the number of help desk requests and ticket closures can be reported.

#### 8.7.1.13 Central Monitoring

The HiWi's operability and performance can be monitored from the redundant NOCs. Failure or serious degradation is detected by NetExpert and will trigger alarms at the NOCs so that a Remedy ticket can be opened and the problem can be corrected expeditiously. The NetExpert software cannot monitor those network portions not administrable by the NOC.

### 8.7.2 Hardware Requirements

#### 8.7.2.1 Materials

T-Mobile will comply with the requirements set forth in the Massport HiWi RFP, Appendix E, Section B, page 1 of 3, Materials.

#### 8.7.2.2 Wireless Network System Equipment

T-Mobile will comply with the requirements set forth in the Massport HiWi RFP, Appendix E, Section B, page 1 of 3, Wireless Network System Equipment.

#### 8.7.2.3 Hardware

##### 8.7.2.3.1 Access Points

T-Mobile will comply with the requirements set forth in the Massport HiWi RFP, Appendix E, Section B, page 1 of 3, Access Points.

##### 8.7.2.3.2 Antennae

T-Mobile will comply with the requirements set forth in the Massport HiWi RFP, Appendix E, Section B, page 1 of 3, Antennae. T-Mobile has no plans for deployment of FHSS antennas.

##### 8.7.2.3.3 Zone Controllers

T-Mobile provides this functionality to control access to its network using two servers in the back-end of its network. The T-Mobile back-end provides accounting and usage statistics for the public network. For private-side applications, we expect to add access controllers to perform this functionality.

##### 8.7.2.3.4 Network Equipment

T-Mobile will comply with the requirements set forth in the Massport HiWi RFP, Appendix E, Section B, page 2 of 3, Network Equipment.

##### 8.7.2.3.5 Special Equipment

T-Mobile will not utilize any special equipment at this time.

##### 8.7.2.3.6 Spares

T-Mobile will typically stocks 10% spare parts at the airport to meet the SLA.

#### 8.7.2.4 Year 2000 Compliance

T-Mobile will fulfill certification requirements with respect to Year 2000 compliance.

#### 8.7.2.5 Power Source

T-Mobile intends to assess power requirements during the site survey. T-Mobile expects power to be provided free of charge since metering at every MDF, IDF, LDF is not practical considering the low power consumption. T-Mobile will run additional power circuits where necessary from nearby electrical panels to the equipment racks. T-Mobile will provide any power conditioning equipment, surge protection, backup power required for reliable operation. Equipment protection will meet ANSI C62.41.

### 8.7.3 Installation Requirements

#### 8.7.3.1 Submittals

The installation of the infrastructure required to provide the public portions of the HotSpot Wireless Internet Service will be implemented to provide coverage with the intent of minimizing radio frequency interference. T-Mobile USA will utilize industry experience in the preparation of a Wireless Internet Site Survey, Design and Implementation Documentation (to include Cable, Power, and Infrastructure drawings), and As-Builts with the purpose of reaching this goal.

The Boston Logan International Airport Site Survey will be incorporated into a Network Design that will encompass AP Mounting Locations, Cable Paths, Riser Diagrams, Telco and Data closet locations, Logical network schematics, Manufacturer specifications and power requirements.

All documentation will be submitted to the Massport Authority in an electronic format utilizing CDROM as the preferred media.

**8.7.3.2 Hardware Installation**

Installation of T-Mobile HotSpot equipment is completed by T-Mobile's Installation Partners. Installation of electrical and cabling is completed by licensed personnel, and is installed per National Electrical Code standards; local electrical and building codes will be adhered to as well.

**8.7.3.3 Software**

T-Mobile USA will provide documentation that details all software in operation in the Boston Logan International Airport HIWI implementation. The list will identify both licensed software or any T-Mobile HotSpot developed Software.

**8.7.3.4 Cable Installation**

All conduit raceways installation for cabling or electrical will be completed in accordance with all Massport Authority Tenant Improvement Guides. T-Mobile will supply final documentation detailing the actual placement specifications upon installation.

**8.7.3.5 Cable Routes/Management**

T-Mobile HotSpot's rack, conduit and cabling is installed and grounded, in accordance with manufacturer's recommend practices and in compliance with the N.E.C.

**8.7.3.6 Shared Infrastructure**

T-Mobile will comply with the Shared Infrastructure requirements as stated in the Massport HiWi RFP, Appendix F, page 2 of 3.

**8.7.3.7 System Configuration Documentation**

T-Mobile will comply with the System Configuration Documentation requirements as stated in the Massport HiWi RFP, Appendix F, page 2 of 3.

**8.7.4 Acceptance Testing Requirements**

**8.7.4.1 Inspection**

T-Mobile will comply with the Inspection requirements as stated in the Massport HiWi RFP, Appendix G, Page 1.

**8.7.4.2 Site Acceptance Test**

T-Mobile will comply with the Inspection requirements as stated in the Massport HiWi RFP, Appendix G, Page 1.

**8.7.4.3 Operator Certification**

T-Mobile will comply with the Inspection requirements as stated in the Massport HiWi RFP, Appendix G, Page 1.

**8.8 Other (h)**

Criteria for the implementation and support of emerging technologies was addressed in Section 8.7.1.1

**8.8.1 Expected Schedule**

The initial deployment for public and private access will be addressed using 802.11b and 802.11a. Other emerging standards cannot be scheduled at this time because they have yet to be ratified. T-Mobile is involved with emerging standards during the standardization process. Once prototype hardware is

available, T-Mobile will evaluate and test product for its quality and security. If the product is found to be commercially viable and has a valid business case, it's scheduled for deployment.

## 9.0 Administration & Reporting Plans

T-Mobile operates a state of the art back office billing and authentication system that enables roaming. Access control is handled in the network via Cisco's Subscriber Session Gateway while session information is recorded and processed in the back office Portal billing system. The capability exists to track roaming partner subscriber sessions by session duration, megabytes transferred, and frequency of session connections. The session data will be captured and roaming settlement will be made on an agreed upon term between the roaming partners. T-Mobile will perform clearing either directly with roaming partners or via an industry-leading clearinghouse.

## 10.0 Confidentiality & Regulatory Matters

T-Mobile is has highest standard of polices and procedures to protect the confidentiality pf subscriber rate, usage and other sensitive information. The subscriber information is currently held in a single source centralized billing system. In this way data confidentiality is maintained. Internally within T-Mobile, access to the system that houses the subscriber information is highly secured and restricted with different levels of access privilege.

Subscriber data is only divulged to the subscriber after verifying privacy details. Should a law enforcement agency request subscriber information, such information will only be disclosed upon T-Mobile's receipt of required legal documents such as a subpoena.

## 11.0 Contract Issues

T-Mobile has carefully reviewed the draft Management and Operating Agreement and has identified concerns, and exceptions regarding the Agreement and Insurance.

Section 1.02: The notion of a Completion Date is not entirely consistent with the Agreement Year concept in the event that completion occurs prior to June 1, 2004. This issue appears throughout the document..

Section 1.13: Gross Revenue needs to acknowledge that by virtue of the nature of our service, it would need to be allocated to the airport based on relative megabyte usage. Also, would seek consideration of other deductions such as bad debt, fraud, chargebacks, refunds, credits, returns, and credits.

Section 3.03: Would seek additional discussion on this as we could have unique offerings that would be available only in our airline partners' clubs and others that would be shown on our website.

Section 5.01: The integration of Terminal E would be contingent upon our review and acceptance as to the network standards, and allow for modifications as required.

Section 5.03: Would seek clarifying language in the final agreement.

Section 6.01, B, 2: Would seek further discussion on calculation of Gross Revenues.

Section 6.04: Would seek thirty-day period in which to remit payments.

Section 6.06: Would seek thirty-day period in which to restore any Security Deposit to its original amount.

Section 7.01 Would seek deletion of the independent auditor requirement.

Section 7.02: Would seek a record retention period of two years instead of six.

Section 7.03: Would seek deletion of this section as T-Mobile has existing internal audit procedures in place and would not establish new internal audit procedures for one site.

Section 7.04: Would seek making books and records available upon receiving thirty days notice rather than 72 hours notice.

Section 8.02: Would request further dialogue with respect to the number of times such activities could be initiated by the Authority.

Section 10.02, Item D: Would seek further dialogue for partial deletion or modification.

Section 10.04: Discussion as to which party would be responsible for absorbing any costs associated with adding Authority as a licensee of Software Licenses at termination of Agreement.

Section 12.01: Changes would be requested in this section in the third paragraph.

Article 13: Would seek changes in sections 13.02, 13.03, 13.05, 13.06 to conform to T-Mobile's insurance practices.

Section 15.01, Item B: Would seek a five-day period rather than 48 hours.

Section 15.01, Item D: Would seek ten-day period rather than three-day period.

Section 17.10: Would seek ability to refer to Airport as a T-Mobile HotSpot on its website and in its sales and marketing collateral.

General. The foregoing represents our major comments to the agreement. Should our proposal be accepted, we would expect to address certain clarifications that we do not consider sufficiently material to mention in this response. We may elect to perform this agreement through a subsidiary of T-Mobile.

**11.1 Service Level**

T-Mobile will have Cisco SmartNet support on equipment. Cisco will be required to provide support 24x7x365 and a 4-hour response. T-Mobile also has a contract with a nationwide company that provide site RF verification, validation, and testing within 4 hours of the initial call during extended business hours.

**12.0 Non-Discrimination & Affirmative Action**

T-Mobile has completed Appendix M, Workforce Composition Form, and the completed form will be found in Attachment 19 of this proposal.

**12.1 Affirmative Action Plan**

We believe that our continued success is dependent on the skills, experiences, and diverse backgrounds that our employees bring to our company. Therefore, we are committed to a strong policy of affirmative action in ensuring equal employment opportunity in all of our employment processes.

While T-Mobile will not be adding staff, either locally or in the Massport area to support this project, Massport can rest assured that we are in compliance with their stated Affirmative Action Policies. A copy of the T-Mobile Affirmative Action Policies can be provided upon request.