Lee County Board Of County Commissioners
Agenda Item Summary **Blue Sheet No.** 20041198

1. REQUESTED MOTION:

ACTION REQUESTED:
Approve implementing a wireless infrastructure, which will allow Lee County to deploy secure wireless access to the Lee County network.

WHY ACTION IS NECESSARY:
Board approval required for the expenditure of approximately $143,000 which is in excess of the $50,000 limit.

WHAT ACTION ACCOMPLISHES:
The wireless infrastructure encompasses software and hardware that will authenticate users and equipment and allow secure access to the Lee County network.

2. DEPARTMENTAL CATEGORY: COMMISSION DISTRICT # C6B	3. MEETING DATE: 09-28-2004

4. AGENDA:	5. REQUIREMENT/PURPOSE: (Specify)	6. REQUESTOR OF INFORMATION:
X CONSENT	___ STATUTE	A. COMMISSIONER
___ ADMINISTRATIVE	___ ORDINANCE	B. DEPARTMENT ITG - INDEPENDENT
___ APPEALS	___ ADMIN. CODE	C. DIVISION ~~Administration~~
___ PUBLIC	___ OTHER	BY: Jim Desjarlais
___ WALK ON		
___ TIME REQUIRED:		

7. BACKGROUND:
Will provide significant productivity improvement at a cost savings of approximately $500,000 per year. The return on investment will be approximately three months.

Funding is available in account KC5132851500 506410 and KC5132851500 503460

8. MANAGEMENT RECOMMENDATIONS:

9. RECOMMENDED APPROVAL:

A Department Director	B Purchasing or Contracts	C Human Resources	D Other	E County Attorney	F Budget Services (Affirm 9/14)			G County Manager
					OA	OM	Risk	GC	
9/13/04				Andrea Fraser 9/13/04	9/13/04	9/14/04	9/14/04	9/15/04	

10. COMMISSION ACTION:

___ APPROVED
___ DENIED
___ DEFERRED
___ OTHER

Rec. by CoAtty
Date: 9/13/04
Time: 11:17
Forwarded To: Budget 9/13/04 11:47am

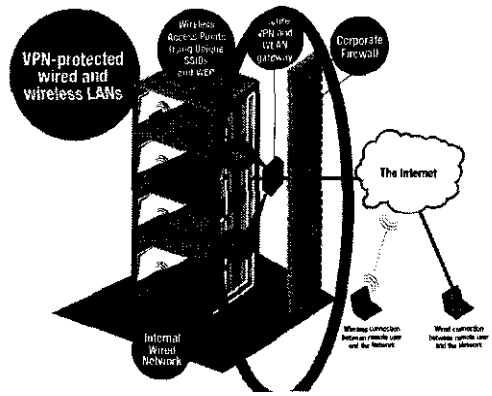
RECEIVED BY COUNTY ADMIN 10
9/13/04
2:05pm SG
COUNTY ADMIN FORWARDED TO: 1L
9.15.04
10:30

Executive summary

Wireless Infrastructure

The Wireless Infrastructure will allow Lee County to deploy secure wireless access for employees in the field.

The wireless infrastructure encompasses software and hardware that will authenticate users and equipment, and allow secure access to Lee County network and information. This infrastructure will protect the networks while enabling the openness of communication and information flow.



Wireless Infrastructure

The benefits realized by a wireless network are:

Productivity improvement. Boosting productivity and efficiency by leveraging existing applications for the employees on the field. Fewer trips back and forth to the office.

- Building Inspectors having wireless access to county applications, e.g. Tidemark, from the field.
- Code Enforcement having access to parcel information from the field.
- Water pumps providing load information to central office. No need for trips to the pumps.
- Fleet personnel having access to inventory when in the field. This will avoid the situation of going back to the office to collect a part and identifying only there that such part was used in another work order.

Cost savings. Reducing costs by providing less expensive means to interact with both employees and customers.

- Reduction on amount of paper filed. Since personnel will have direct access to the applications.
- Reduce cost of deployment of hardware for new employees.
- Capability to deploy citizen self-service kiosks without need of wiring buildings and locations.

Information accuracy. Increased accuracy of data entry, since it will be performed one time, by the professional that is collecting the data.

Improved communications. Field employees will have access to e-mail and internet at any location, not needing to go back to their desks for retrieving e-mails or data.

Wireless ROI

# of Employees		2300
# of Desktops		1800
# of Laptops		200
Employees that can benefit from WLAN		50
Productivity gain per week (hours)		10
Weeks worked per year		48
Average fully burdened salary per hour		23.01
Productivity Savings per year	**$**	**552,240**
Annual Support cost	$	18,269
Wireless Infrastructure Capital Expense	$	114,394
Access Cards, Access Points	$	10,000
Total Expense	**$**	**142,663**
ROI		**3.10 months**

Lee County Wireless Infrastructure
Required Core Network Upgrades

September 13, 2004

1. Executive Summary

This proposal makes recommendations regarding the upfront core network infrastructure upgrades that are required before Lee County can implement any of the various wireless networking initiatives that are being requested by various departments within the county. These upfront upgrades are necessary to ensure reliable and secure wireless connections to the county network that can be supported. Cost breakdown is as follows:

Software Cost	Hardware Cost	Annual Support Cost	Total	Implementation (Man Hours)
$14,738.85	$109,655.20	$18,269.45		310 hours
		TOTAL	**$142,663.50**	

The second section describes these upgrades, and the last section is a review of the various projects that are presently being requested by or evaluated for various departments within Lee County. The upgrades in this document are required before any of these projects can be implemented.

Please note that these upgrades, as described here, are for the core network infrastructure upgrades that are required to ensure consistent and secure connections to the network. As the projects described in section 3 below are rolled out, more upgrades to the specific location's Local Area Network (LAN) will be required at additional expense. These costs will include the various access points, possible power-over-ethernet additions to the LAN equipment at the site, and other required upgrades. These costs should be incurred on a case-by-case basis, at the department level, as the various wireless initiatives are designed, approved and implemented.

More information on the full wireless infrastructure recommendation to Lee County is available in the document "*ITG Wireless Infrastructure Recommendation.*" This document details the methodology that Atos Origin / Lee County ITG has chosen to adopt as the best practice for implementing wireless infrastructures. It also describes in detail the full recommendation on implementing wireless technologies that connect to the county's network, including discussing "Wireless Fidelity" (Wi-Fi hotspots), "Third Generation" (3G) connectivity to the network, and other details.

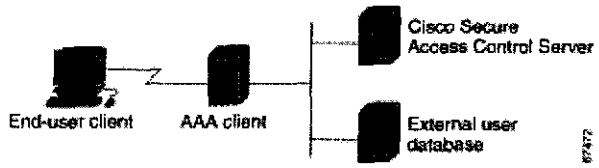
2. Atos Origin / ITG Recommendations

2. 1 Required Core Infrastructure Security Additions

2.1.1 Setup AAA (CiscoSecure ACS) server for user authentication

CiscoSecure Access Control Server, or "CiscoSecure ACS", provides authentication, authorization, and accounting (AAA—pronounced "triple A") services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. The AAA client in the scenario below represents any such device that provides AAA client functionality and uses one of the AAA protocols supported by CiscoSecure ACS.

2.1.1.1 Simple AAA Scenario



CiscoSecure ACS centralizes access control and accounting, in addition to router and switch access management. With CiscoSecure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the external user database shown above is optional, support for many popular user repository implementations enables companies to put to use the working knowledge gained from and the investment already made in building their corporate user repositories.

2.1.1.2 Technical Specifications and Cost Estimates for AAA Server Implementation

CiscoSecure ACS supports Cisco AAA clients such as the Cisco 2509, 2511, 3620, 3640, AS5200 and AS5300, AS5800, the Cisco PIX Firewall, Cisco Aironet Access Point wireless networking devices, Cisco VPN 3000 Concentrators, and Cisco VPN 5000 Concentrators. It also supports third-party devices that can be configured with the Terminal Access Controller Access Control System (TACACS+) or the Remote Access Dial-In User Service (RADIUS) protocol. CiscoSecure ACS treats all such devices as AAA clients. CiscoSecure ACS uses the TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment.

No server cost is presented here because an existing server will be used to setup the AAA (CiscoSecure) application.

Qty.	Part #	Hardware / Software Description	Price	Ext. Price
1	CSACS-3.2-WIN-K9	CiscoSecure ACS 3.2 for Windows (Sfw)	4,076.60	4,076.60
1	CON-SAS-CSACS-3.2	SAS SVC, CiscoSecure ACS 3.2 for Windows (Svc)	1,139.05	1,139.05
1	CSURT-1102-K9	Starter Kit; User Reg Tool 2.5 SW, 1102 (Hdw)	16,996.60	16,996.60
1	CON-SAS-URT2.5	SAS SVC., Config. Option; Mandatory URT 2.5 software (Sfw)	2,849.05	2,849.05
1	CON-SNT-URT1102	SMARTNET 8X5XNBD Starter Kit; User Re (Svc)	760.00	760.00
		TOTALS...	**25,821.30**	**25,821.30**

2.1.2 Setup an IDS (Intrusion Detection System) to detect when a security breach has occurred

2.1.2.1 Technical Specifications and Cost Estimates for IDS Implementation

It is recommended that the Cisco IDS 4200 Series sensors be used for the IDS solution. These intrusion detection system sensors work in concert with the other components to efficiently protect our data and information infrastructure. With the increased complexity of security threats, achieving

efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

The sensor will be connected to new blades on each of the 3 main core downtown switches in the Lee County network. The costs are for the blades to handle the new sensor, as well as the sensor itself, are:

Qty.	Part #	Description	Price	Ext. Price
3	WS-SVC-IDS2BUNK9=	IDSM-2 600M mod	20,396.60	61,189.80
3	CON-OSP-IDSBNK9	ONSITE 24X7X4 IDSM-2 600M mod	4,559.05	13,677.15
1	IDS-4215-K9	Cisco IDS 4215 Sensor, 80-Mbps	4,960.60	4,960.60
1	CON-SNT-IDS4215	SMARTNET 8X5XNBD Cisco IDS 4215 Sensor, 80-Mbps	554.80	554.80
		Totals...	**30,471.05**	**80,382.35**

2.1.3 Setup LDAP to integrate our existing user database for authentication

The authentication portion of CiscoSecure ACS is called Radius. Integrating an application such as LDAP into Radius will allow for more streamlined and controlled access to the network. LDAP, which stands for "Lightweight Directory Access Protocol", is a phone-book type application that would allow for central management of all user information in the county, such as name, department, phone number, email address, etc. This type of application is commonly used by many applications for authentication, including the wireless applications described here.

If an authentication attempt fails against its internal list of users, the CiscoSecure ACS will try the selected databases configured in the Unknown User Policy. The external databases are attempted sequentially, in the configured order. Upon a successful attempt, the user is added to the CiscoSecure ACS internal database but marked for authentication by the appropriate database. For subsequent authentication attempts, CiscoSecure ACS will try the supplied credentials directly against the previously successful external database.

NOTE - This step could be implemented later, if time constraints keep it from being implemented initially. The LDAP integration to CiscoSecure ACS is a recommended best-practice, but the CiscoSecure ACS database of allowed users could be manually setup in advance, containing only those county employees who are authorized to use the wireless networking functionality.

There are no additional costs associated with LDAP software, as it is already part of the Novell file-and-print services that the county uses. LDAP will be setup on an existing server, so no additional hardware expense would be incurred.

2.1.4 Additional modules for CiscoWorks to enhance managing network components

CiscoWorks VPN/Security Management Solution (VMS) is an integral element of the SAFE Blueprint for Enterprise Network Security from Cisco, and contributes to organizational productivity by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, network intrusion detection systems (IDS), and host intrusion prevention systems. Integrated with other CiscoWorks products, CiscoWorks VMS also includes network device inventory, change audit, and software distribution features.
CiscoWorks VMS 2.2 provides the security management for our overall security needs. It includes the following applications, organized by functional area:

- **Firewall management** - Enables the large-scale deployment of Cisco firewalls. Smart Rules is an innovative feature that allows a security policy to be consistently applied to all firewalls. Smart Rules allows a user to define common rules once, reducing configuration time and resulting in fewer administrative errors.
- **Network IDS management** - Offers efficient deployment of hundreds of sensors using group profiles. Additionally, powerful signature management helps to increase the accuracy and specificity of detection.
- **Host intrusion prevention system management** - Scalable to thousands of endpoints per manager to support large enterprise deployments. The open and extensible architecture offers the capability to define and enforce security according to corporate policy. Offers "zero update" prevention for known and unknown attacks.
- **VPN router management** - Provides functions for the setup and maintenance of large deployments of VPN connections and Cisco IOS firewalls on Cisco security routers and Cisco Catalyst 6000 VPN service modules.
- **Security monitoring** - Provides integrated monitoring to help administrators have a comprehensive view of security across the network, with event correlation to detect threats not apparent with individual events. See
- **Performance monitoring** - Provides functions for monitoring and troubleshooting services that contribute to enterprise network security.
- **VPN monitoring** - Allows network administrators to collect, store, and view information on IP Security VPN connections for remote-access or site-to-site VPN terminations.
- **Operational management** - Allows network managers to build a complete network inventory, report on hardware and software changes, and manage software updates to multiple devices.

Lee County currently owns CiscoWorks software, but in order to implement these new modules, additional charges will be incurred.

- Replacement server would need to be purchased at a cost of $8,355 to load the entire CiscoWorks application onto. The current server is inadequate to run all the additional modules.
- The additional modules themselves will cost $5,776.60 total upfront.
- Presently the county is already paying annual maintenance of $7,600 for CiscoWorks software. These additional modules will cost $1,226.45 more per year.

Qty.	Part #	Description	Price	Ext. Price
1	Dell Standard Svr	Dell Standard Server	8,355.00	8,355.00
1	CWWLSE-1130-K9	Wireless LAN Solution 2.5 (Hardware and Software included)	5,776.60	5,776.60
1	CON-SNT-CWLSE1130	8x5xNBD Svc, Wireless LAN Sol. 2.0	258.40	258.40
1	CON-SAS-CWWLSE-20	SW APP SUPP CWWLSE-2.0 SW	968.05	968.05
		TOTALS...	**15,358.05**	**15,358.05**

2.1.5 Install VPN Concentrators

To allow for certain types of recommended wireless connections to the network, it will be necessary to install hardware VPN solution into the network. This type of solution is described in detail in the "*ITG Wireless Infrastructure Recommendation*" document, and is part of the upfront requirements for wireless connectivity.

Qty.	Part #	Description	Price	Ext. Price
1	CVPN3020E-RED-K9	VPN3020:Chassis, 3FE, 2SEP-E, 750 user, client, 2 PWR	8,153.20	8,153.20
1	CVPN3020-SW-K9	VPN3020:SW	2,036.60	2,036.60
1	CON-SNT-3020RDB	SMARTNET 8X5XNBD 3020 750usrs,2PS, 2S	912.00	912.00
		Totals...	**11,101.80**	**11,101.80**

2.1.6 Upgrade Cisco Device's Operating Systems as required

In conjunction with implementation of the wireless infrastructure upgrades, software upgrades to various Cisco devices' operating systems will also be required. There are no additional costs for these upgrades, as they are included in the annual hardware and software maintenance that the county pays to Cisco. It is estimated that these upgrades will take approximately 30 days to fully implement, with working off-hours a requirement.

2.1.7 Cost Recap for Core Infrastructure Upgrade Costs

Application/Option	Software Cost	Hardware Cost	Annual Support Cost	Implementation (Man Hours)
2.1.1 AAA Server (Cisco ACS)	$6,925.65	$16,996.60	$1,899.05	60
2.1.2 IDS (Intrusion Detection) Options				
Internet Edge Stand alone device	Incl.	$4,960.60	$554.80	10
Three Core Router devices	Incl.	$61,189.80	$13,677.15	30
2.1.3 LDAP integration to Radius	$0.00	$0.00	$0.00	30
2.1.4 CiscoWorks modules for Windows and Unix (Wireless LAN Solution version 2.5 includes these modules)	** $0.00	$8,355.00	*** $0.00	
Firewall Management	Incl.			20
IDS Management	Incl.			30
VPN Router Management	Incl.			20
Security Monitor	Incl.			20
Performance Monitor	Incl.			10
VPN Monitor	Incl.			10
Operational Management	Incl.			10
Additional module costs and maintenance...	$5,776.60		$1,226.45	
2.1.5 Install VPN Concentrator	$2,036.60	$ 8,153.20	$912.00	30
2.1.6 Upgrade Cisco Devices' Operating Systems				30
Access cards and access points		$10,000		
Total	**$14,738.85**	**$109,655.20**	**$18,269.45**	**310**
** Software already owned by Lee County, therefore no additional charges incurred.				
*** Software maintenance currently being paid on CiscoWorks software is $7,600, which is not included in these charges.			**Grand total**	**$142,663.50**

3. Lee County Wireless Projects

3.1 Pending Lee County Wireless Projects

Department	Project	Description
Community Development	DCD Field Force Automation	To provide wireless field force automation to Community Development (Code Enforcement and Inspectors)
Library	Wireless Training Cart	A cart containing laptops what will be wirelessly connected to the network. The lab will be moved to different locations in the library to provide training facilities
Utilities	Wireless Network Connections	To wirelessly connect devices to the network for Utility department staff
DOT	Wireless Network Connections	To wirelessly connect devices to the network for DOT department staff (same requirements as for Utilities)
Community Development	Environmental Violation (PERT) - Wireless Access	Research and implement project tracking software for the organization. Create application to do all field work online using palm pilot / laptops and connect to PERT and Tidemark databases.

3.2 Strategic Lee County Wireless Projects

Department	Project	Description
County Wide	Information for All	Provide access to internet and IT strategies to citizens and minorities.
County Wide	Field Force Automation	Enable employees to work remotely accessing the network wirelessly.
County Wide	Information Kiosks	Enable wireless kiosks to be used by citizens in county facilities.