

Item # 4-4E

City of Carson City
Agenda Report

Date Submitted: June 12, 2007

Agenda Date Requested: June 21, 2007
Time Requested: Consent

To: Mayor and Supervisors

From: Purchasing & Contracts

Subject Title: Action to approve Intrastate Interlocal Contract between Public Agencies, a Contract between the State of Nevada Department of Information Technology (DoIT) and Carson City Information Technology, to provide "SilverNet" the State of Nevada's enterprise digital wide area network operated by DoIT at a cost of \$357.70 per month through June 30, 2008 and \$386.57 per month through June 30, 2009 from the General Fund (File 0708-023)

Staff Summary: The City's connections to the State SilverNet network have become a vital part of the City's overall data communications infrastructure. This alliance with the State affords the City tremendous flexibility and opportunity and is becoming more important as our relationships with State agencies grow.

Type of Action Requested: (check one)
 Resolution Ordinance
 Formal Action/Motion Other (Specify)

Does This Action Require A Business Impact Statement: Yes No

Recommended Board Action: I move to approve Intrastate Interlocal Contract between Public Agencies, a Contract between the State of Nevada Department of Information Technology (DoIT) and Carson City Information Technology, to provide "SilverNet" the State of Nevada's enterprise digital wide area network operated by DoIT at a cost of \$357.70 per month through June 30, 2008 and \$386.57 per month through June 30, 2009 from the General Fund (File 0708-023)

Explanation for Recommended Board Action: NRS 277.180 authorizes a public agency to contract with any other public agency to perform any governmental service, activity or undertaking which any of the public agencies entering into the contract is authorized by law to perform.

This contract provides the City with many benefits that include:

- low cost,
- access to the State's SilverNet network,

- fiber connections between two City locations and the State,
- high speed Internet access,
- firewall security services,
- network monitoring and diagnostics, and
- networking and security consultation services.

DoIT requires that Carson City first obtains approval of the Contract from the Board of Supervisors, then provide DoIT five (5) signed original Contracts for them to process, and then they will provide us two (2) signed original Contracts for our files.

Applicable Statute, Code, Policy, Rule or Regulation: NRS 277.180

Fiscal Impact: \$4,292.40 General Fund Automation Telephone for FY 0708 and \$4,638.84 General Fund Automation Telephone for FY 0809


Explanation of Impact: \$4,292.40 General Fund Automation Telephone for FY 0708 and \$4,638.84 General Fund Automation Telephone for FY 0809


Funding Source: General Fund Automation Telephone FY 0708 & FY 0809

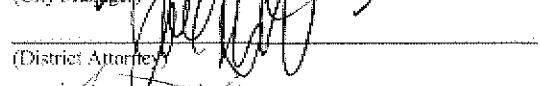
Supporting Material: Intrastate Interlocal Contract Between Public Agencies

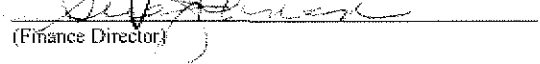
Prepared By: Cheryl Adams, Purchasing & Contracts Manager

Reviewed By:


 Information Technology


 (City Manager)


 (District Attorney)


 (Finance Director)

Date: 6/12/07
 Date: 6/12/07
 Date: 6/12/07
 Date: 6/12/7

Board Action Taken:

Motion: _____ 1) _____ Aye/Nay
 _____ 2) _____

 (Vote Recorded By)

INTRASTATE INTERLOCAL CONTRACT BETWEEN PUBLIC AGENCIES

A Contract Between the State of Nevada
Acting By and Through Its

Department of Information Technology
400 W. King St., Suite 300
Carson City, Nevada, 89703-4204
Phone: 775-684-5800 Fax: 775-684-5846
(Henceforth known as "DoIT")

And

Carson City Information Technology
201 North Carson Street, Suite #7
Carson City, Nevada, 89701
Phone: 775-887-2160 Fax: 775-887-2288
(Henceforth known as "Carson City")

WHEREAS, NRS 277.180 authorizes any one or more public agencies to contract with any one or more other public agencies to perform any governmental service, activity or undertaking which any of the public agencies entering into the contract is authorized by law to perform; and

WHEREAS, it is deemed that the services of DoIT hereinafter set forth are both necessary to Carson City and in the best interests of the State of Nevada; and

WHEREAS, NRS 242.141 Authorizes DoIT to provide service for agencies not under the control of the Governor, upon the request of any such agency. If there are sufficient resources available to the Department, it may provide services to counties, cities and towns and to their agencies.

NOW, THEREFORE, in consideration of the aforesaid premises, the parties mutually agree as follows:

1. **REQUIRED APPROVAL.** This Contract shall not become effective until and unless approved by the Nevada State Board Of Examiners and appropriate official action of the governing body of each party.
2. **DEFINITIONS.** "State" means the State of Nevada and any State agency identified herein, its officers, employees and immune contractors as defined in NRS 41.0307. "DoIT" specifically indicates the Department of Information Technology and its authorized agents. "Customer" means requesting county, city or authorized agent. "SilverNet" means the State of Nevada's enterprise digital wide area network operated by DoIT.
3. **CONTRACT TERM.** This Contract shall be effective **from July 1, 2007** subject to approval of the State Board of Examiners to **June 30, 2009**, unless sooner terminated by either party as set forth in this Contract.
4. **TERMINATION.** This Contract may be terminated by either party prior to the date set forth in paragraph (3), provided that a termination shall not be effective until 30 days after a party has served written notice upon the other party. This Contract may be terminated by mutual consent of both parties or unilaterally by either party without cause. The parties expressly agree that this Contract shall be terminated immediately if for any reason State and/or Federal funding ability to satisfy this Contract is withdrawn, limited, or impaired.

5. NOTICE. All notices or other communications required or permitted to be given under this Contract shall be in writing and shall be deemed to have been duly given if delivered by any delivery or courier service personally in hand, by telephonic facsimile with simultaneous regular mail, or mailed certified mail, return receipt requested, postage prepaid on the date posted, and addressed to the other party at the address set forth above.

6. INCORPORATED DOCUMENTS. The parties agree that the services to be performed shall be specifically described; this Contract incorporates the following attachments in descending order of constructive precedence:

- ATTACHMENT A: SPECIFICATIONS AND SERVICE OPTIONS
- ATTACHMENT B: STATE OF NEVADA IT SECURITY POLICY
- ATTACHMENT C: DEPARTMENT OF INFORMATION TECHNOLOGY WIRELES NETWORK 802.11 STANDARD
- ATTACHMENT D: BILLING

7. CONSIDERATION. The State of Nevada, Department of Information Technology agrees to provide the services set forth in paragraph (6) at a cost of **\$357.70 per month in FY08** for Tier 2 SilverNet services and a cost of **\$386.57 per month in FY09** also for Tier 2 SilverNet services. The total Contract amount shall not exceed **\$8,931.24: \$4,292.40 for FY08 and \$4,638.84 for FY09**. This cost is based on bandwidth utilization averaged over an entire fiscal biennium and does not change from month to month.

8. ASSENT. The parties agree that the terms and conditions listed on incorporated attachments of this Contract are also specifically a part of this Contract and are limited only by their respective order of precedence and any limitations expressly provided.

9. INSPECTION & AUDIT.

a. Books and Records. Each party agrees to keep and maintain under general accepted accounting principles full, true and complete records, agreements, books, and documents as are necessary to fully disclose to the other party, the State or United States Government, or their authorized representatives, upon audits or reviews, sufficient information to determine compliance with all State and Federal regulations and statutes.

b. Inspection & Audit. Each party agrees that the relevant books, records (written, electronic, computer related or otherwise), including but not limited to relevant accounting procedures and practices of the party, financial statements and supporting documentation, and documentation related to the work product shall be subject, at any reasonable time, to inspection, examination, review, audit, and copying at any office or location where such records may be found, with or without notice by the other party, the State Auditor, The Department of Information Technology Office of Information Security, Employment Security, the Department of Administration, Budget Division, the Nevada State Attorney General's Office or its Fraud Control Units, the State Legislative Auditor, and with regard to any federal funding, the relevant federal agency, the Comptroller General, the General Accounting Office, the Office of the Inspector General, or any of their authorized representatives.

c. Period of Retention. All books, records, reports, and statements relevant to this Contract must be retained by each party for a minimum of three years and for five years if any federal funds are used in this Contract. The retention period runs from the date of termination of this Contract. Retention time shall be extended when an audit is scheduled or in progress for a period reasonably necessary to complete an audit and/or to complete any administrative and judicial litigation which may ensue.

10. BREACH; REMEDIES. Failure of either party to perform any obligation of this Contract shall be deemed a breach. Except as otherwise provided for by law or this Contract, the rights and remedies of the parties

shall not be exclusive and are in addition to any other rights and remedies provided by law or equity, including but not limited to actual damages, and to a prevailing party reasonable attorneys' fees and costs. It is specifically agreed that reasonable attorneys' fees shall include without limitation \$125 per hour for State-employed attorneys.

11. LIMITED LIABILITY. Any and all liability of DoIT for damages or claims under this contract will be limited to prorated charges on a daily basis while service is not provided by DoIT. The parties will not waive and intend to assert available NRS Chapter 41 liability limitations in all cases. Contract liability of both parties shall not be subject to punitive damages. To the extent applicable, actual contract damages for any breach shall be limited by NRS 353.260 and NRS 354.626.

12. FORCE MAJEURE. Neither party shall be deemed to be in violation of this Contract if it is prevented from performing any of its obligations hereunder due to strikes, failure of public transportation, civil or military authority, act of public enemy, accidents, fires, explosions, or acts of God, including, without limitation, earthquakes, floods, winds, or storms. In such an event the intervening cause must not be through the fault of the party asserting such an excuse, and the excused party is obligated to promptly perform in accordance with the terms of the Contract after the intervening cause ceases.

13. INDEMNIFICATION.

a. To the fullest extent of limited liability as set forth in paragraph (11) of this Contract, each party shall indemnify, hold harmless and defend, not excluding the other's right to participate, the other from and against all liability, claims, actions, damages, losses, and expenses, including but not limited to reasonable attorneys' fees and costs, arising out of any alleged negligent or willful acts or omissions of the party, its officers, employees and agents. Such obligation shall not be construed to negate, abridge, or otherwise reduce any other right or obligation of indemnity which would otherwise exist as to any party or person described in this paragraph.

b. The indemnification obligation under this paragraph is conditioned upon receipt of written notice by the indemnifying party within 30 days of the indemnified party's actual notice of any actual or pending claim or cause of action. The indemnifying party shall not be liable to hold harmless any attorneys' fees and costs for the indemnified party's chosen right to participate with legal counsel.

14. INDEPENDENT PUBLIC AGENCIES. The parties are associated with each other only for the purposes and to the extent set forth in this Contract, and in respect to performance of services pursuant to this Contract, each party is and shall be a public agency separate and distinct from the other party and, subject only to the terms of this Contract, shall have the sole right to supervise, manage, operate, control, and direct performance of the details incident to its duties under this Contract. Nothing contained in this Contract shall be deemed or construed to create a partnership or joint venture, to create relationships of an employer-employee or principal-agent, or to otherwise create any liability for one agency whatsoever with respect to the indebtedness, liabilities, and obligations of the other agency or any other party.

15. WAIVER OF BREACH. Failure to declare a breach or the actual waiver of any particular breach of the Contract or its material or nonmaterial terms by either party shall not operate as a waiver by such party of any of its rights or remedies as to any other breach.

16. SEVERABILITY. If any provision contained in this Contract is held to be unenforceable by a court of law or equity, this Contract shall be construed as if such provision did not exist and the nonenforceability of such provision shall not be held to render any other provision or provisions of this Contract unenforceable.

17. ASSIGNMENT. Neither party shall assign, transfer or delegate any rights, obligations or duties under this Contract without the prior written consent of the other party.

18. OWNERSHIP OF PROPRIETARY INFORMATION. Unless otherwise provided by law or this Contract, any reports, histories, studies, tests, manuals, instructions, photographs, negatives, blue prints, plans, maps, data, system designs, computer code (which is intended to be consideration under this Contract), or any other documents or drawings, prepared or in the course of preparation by either party in performance of its obligations under this Contract shall be the joint property of both parties.

19. PUBLIC RECORDS. Pursuant to NRS 239.010, information or documents may be open to public inspection and copying. The parties will have the duty to disclose unless a particular record is made confidential by law or a common law balancing of interests.

20. CONFIDENTIALITY. Each party shall keep confidential all information, in whatever form, produced, prepared, observed or received by that party to the extent that such information is confidential by law or otherwise required by this Contract.

21. PROPER AUTHORITY. The parties hereto represent and warrant that the person executing this Contract on behalf of each party has full power and authority to enter into this Contract and that the parties are authorized by law to perform the services set forth in paragraph (6).

22. GOVERNING LAW; JURISDICTION. This Contract and the rights and obligations of the parties hereto shall be governed by, and construed according to, the laws of the State of Nevada. The parties consent to the jurisdiction of the Nevada district courts for enforcement of this Contract.

23. ENTIRE AGREEMENT AND MODIFICATION. This Contract and its integrated attachment(s) constitute the entire agreement of the parties and such are intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Unless an integrated attachment to this Contract specifically displays a mutual intent to amend a particular part of this Contract, general conflicts in language between any such attachment and this Contract shall be construed consistent with the terms of this Contract. Unless otherwise expressly authorized by the terms of this Contract, no modification or amendment to this Contract shall be binding upon the parties unless the same is in writing and signed by the respective parties hereto, approved by the State of Nevada Office of the Attorney General.

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be signed and intend to be legally bound thereby.

 Carson City Signature Date

 Title

 Director/CIO

 Department of Information Technology Date
 Signature

 Title

 Signature – Nevada State Board of Examiners

APPROVED BY BOARD OF EXAMINERS

Approved as to form by:

On _____
 (Date)

 Deputy Attorney General for Attorney General,
 State of Nevada

On _____
 (Date)

SPECIFICATIONS AND SERVICE OPTIONS

Section I: Specifications and Standards

- 1.1 **Routers:** All connections will require a CISCO router for intranet connectivity.
- 1.2 **Line Configurations:** All T-1 circuits will be defined as Extended Super Frame (ESF) and Bipolar 8 Zero Substitution (B8ZS).
- 1.3 **Network Addressing:** Network Address Translation or Port Address Translation (NAT/PAT) will be used as required to address security issues and maintain SilverNet network integrity within the SilverNet administrative domain (AD).
- 1.4 **IP addressing:** IP addressing for NAT and PAT configurations into SilverNet will be supplied by DoIT.
- 1.5 **Routing Protocols:** SilverNet supports Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Internet Protocol Version 6 (IPv6) and static routes only.

Section II: City of Carson Responsibilities

- 2.1 *City of Carson will conform to State network and security standards while connected in accordance with the State's Security Policy. The City of Carson is responsible for its own additional requirements for security.*
- 2.2 Internet access is without content restrictions other than Peer to Peer (P2P) and Instant Messaging. Acceptable use policies and procedures are the responsibility of the City of Carson. The acceptable use policies of the State must be used as a minimum guideline for Internet access.
- 2.3 *City of Carson must provide the appropriate, secure, climate-controlled space to accommodate DoIT transport and/or network interface equipment.*
- 2.4 If desired, a Business Service Level Agreement will be developed jointly between the City of Carson and DoIT. The Business SLA will focus on the business service requested; however, all parties will ensure network management issues, if any, are addressed in the context of the service requested. The City of Carson will track and manage the Business SLA, and inform DoIT of any significant network connectivity changes.

Section III: DoIT Responsibilities

- 3.1 DoIT will install, maintain, repair and upgrade network and transport equipment owned and operated by DoIT as required in maintaining operational integrity of connection for 24x7 operational availability.
- 3.2 Exceptions:
 - 3.2.1 DoIT operates a standing maintenance window for core network related upgrades and enhancements. The SilverNet maintenance window is every Wednesday from 9PM to 2AM. Normal maintenance may result in short-term outages. Maintenance outages are posted in advance on the SilverNet Web server accessible to City of Carson. In addition the DoIT will provide bandwidth utilization graphs available on the SilverNet Web server.

3.2.2 Emergency Maintenance: Core network code and hardware failures are considered emergency maintenance and are dispatched immediately.

3.3 DoIT reserves the right to terminate any service at any time as a result of security breaches or activity that compromises the integrity of SilverNet or places any other City of Carson or State agencies at risk.

Section IV: Configuration

4.1 DoIT will provide provisioning, configuration and operational maintenance of all communications equipment to the customer's network demarcation. Procurement of hardware, maintenance and telecommunications and access charges will be the responsibility of City of Carson.

4.1.1 DoIT will ensure service to the outbound port of the DoIT firewall/router port or the last point of State-owned transport.

Note: All connectivity operations past the State's demarc will be the responsibility of the City of Carson.

Section V: Transport

5.1 Microwave Transport: Communications will be established over the DoIT microwave system. Data speeds for service are: T-1, 1.544Mbps or greater if based upon system availability.

5.1.1 This service is available to county seats that have the State microwave system spurs installed.

5.1.2 DoIT will provide end point termination to location of county spur termination point.

5.2 Leased Service: Communications service will be established over a private leased line through a qualified telecommunications provider. Data rates: T-1, 1.544Mbps, ATM, Variable Rate Frame Relay and Digital Subscriber Line (DSL).

5.2.1 All options are not available in all areas; DoIT can recommend options suitable to specific locations.

5.2.2 Operations are dependent on service configurations defined in Section IV.

5.3 Fiber Optic Cable: Communications will be provided utilizing the DoIT managed fiber optic infrastructure. Data rates for service are: 100Mbps and 1000Mbps.

5.3.1 Fiber option is not available in all areas; DoIT can recommend options suitable to specific locations.

5.3.2 DoIT will provide lit fiber and interface specifications for operations.

5.4 Virtual Private Network (VPN) & Wireless: Communications will be made utilizing an Internet service provider. Supported data rates 56Kbs~3Mbps.

5.4.1 Each user will be issued a user ID, password and security connectivity software (one account per person) in accordance with State security policies and procedures. VPN service is provided to the City of Carson at an additional cost of \$5.88 per month, per user in FY08 and \$6.04 per month, per user in FY09.

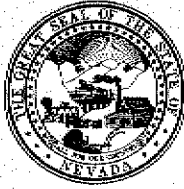
- 5.4.2 Wireless bridging to existing spur or hub nodes must follow the Department of Information Technology 802.11 Wireless Standard Control No. 54-09 revision C. All exceptions must submit to and reviewed by the Office of Information Security.

Section VI: SilverNet Service Options

- 6.1 SilverNet Access: This basic service provides access to multiple state agencies via SilverNet. Connectivity to include HOST ACCESS, USER ID and LOGON operations will be negotiated between DoIT and City of Carson. Final approval and authorization will be determined and approved by DoIT.
- 6.1.1 Each approving authority will provide a letter of authorization to DoIT indicating access to be permitted through the State firewall. Letters of authority and access will become attachments to the principal Interlocal agreement. (Other supporting sections; Business SLAs refer to Section 2.4.)
- 6.2 Enhanced SilverNet Access: Same as Section 6.1 but also includes City of Carson tailored access control lists, enhanced connection monitoring and LAN security administration assistance.
- 6.2.1 Subject to a security needs assessment/risk analysis.
- 6.3 Internet access utilizing the State firewall service: DoIT operates and maintains enterprise firewall services. Internet connectivity will require a design and review process to establish mutual security guidelines that can be met.
- 6.3.1 City of Carson traffic will access the Internet utilizing State of Nevada IP address block.
- 6.4 Unprotected Internet Feed: A dedicated connection to the State ingress router(s) providing the City of Carson with network routing service to the Internet.
- 6.4.1 City of Carson must use either Network Address Translation (NAT) or port address translation (PAT) or obtain their own network address space.
- 6.4.2 Same as Section 6.4.1, subject to a security needs assessment/risk analysis.

Section VII: BACKUP CIRCUITS

- 7.1 It is understood that from time to time, brief service outages lasting less than one (1) business day may occur. These outages fall into the following categories:
- 7.1.1 DoIT equipment and/or transport outages. When DoIT is responsible for any interruption of services under this Contract, the liability of DoIT is limited to prorated daily charges when DoIT service outages lasting longer than one (1) business day occur. Brief outages lasting less than one (1) day will not be the basis of any claims against DoIT.
- 7.1.2 Public telecommunications provider equipment and/or transport outages. When public telecommunications providers are responsible for outages, the City of Carson is responsible for seeking compensation from the providers responsible. Outages due to any fault of public telecommunications providers will not be the basis of any claims against DoIT.
- 7.2 DoIT can recommend options to help keep transport service or limited service available in the event of a transport failure. This would not cover the failure of network hardware or components but would provide an alternate path in the event of a transport outage.



State of Nevada

Information Technology Security Committee

Policy

Control No.	Rev.	Title	Effective Date	Page
4.02	A	IT Security Policy	02/14/2002	1 of 4

1.0 PURPOSE

This policy establishes a minimum information technology (IT) security policy for the protection of State assets inclusive of information, computers and networks. The intent of IT is to ensure the availability of timely, accurate information for the delivery, of services and products to the citizens of the State of Nevada.

The protection of State IT requires an approach that will result in implementation of balanced, cost-effective security disciplines and techniques commensurate with the identified risks and threats to the organization and its information technology.

The IT security policy and subsequent standards provide the minimum high-level policy and standards designed to provide a broad direction for protecting State IT assets. The State IT Security Committee, whose membership consists of representatives from multiple state departments and/or divisions have developed these policies and supporting IT Security Standards and Guidelines.

2.0 SCOPE

This policy and all State IT security standards adopted in support of this policy apply to all Executive Branch departments, including divisions, bureaus, boards and commissions, regardless of physical location, that operate, manage or use IT services or equipment. The scope includes:

- A. The operation, management or use of stand-alone, shared or network-attached computers.
- B. The operation, management, or use of data, telecommunications equipment, networks, or services.
- C. Purchased computer services or telecommunication network services from other state entities or commercial concerns.
- D. Contract or vendor personnel engaged with a State entity to provide services that require use of State information technology, which includes hardware, software, application systems, network and data.
- E. All users of State information technology. Security for IT resources provided for use by the general public must be written and kept separate from the agency's security policies, standards and procedures.

3.0 EFFECTIVE DATES

The requirements of this policy are effective 90 days after sign-off by the Governor or his designee.



State of Nevada

Information Technology Security Committee

Policy

Control No.	Rev.	Title	Effective Date	Page
4.02	A	IT Security Policy	02/14/2002	2 of 4

4.0 RESPONSIBILITIES

- A. The State IT Security Committee is responsible for establishing policies, standards and guidelines for IT Security and providing them to agency management.
- B. Agency management is accountable for the protection of State assets, including IT relating to the conduct of State business. Each employee has the responsibility and must protect the IT assets and information from unauthorized modification, destruction or disclosure.

5.0 RELATED DOCUMENTS

- NRS 242.111 Information Technology – Regulations
- NRS 242.115 Duties of Planning and Research

And in compliance with Federal laws specifically:

- Public Law 100-235 Computer Security Act of 1987
- OMB Circular A-130 Security of Federal Automated Systems

6.0 POLICIES

6.0.1 SECURITY MANAGEMENT:

- A. Department heads are responsible for the security of their information technologies and for establishing security controls on a department wide basis. The departments shall ensure that:
 - 1) An IT Security Plan(s) is developed commensurate with the sensitivity and value of the information processed and maintained, the need for continued operation of critical business functions and the level of risks and magnitude of loss or harm that could result from the loss, misuse, disclosure or modification of the IT assets.
 - 2) IT Security awareness and training is provided to all agency staff at least annually.
 - 3) New employee orientation is established to introduce IT Security policies, standards and procedures.
 - 4) IT Contingency Plans, including appropriate data and system backup and recovery procedures are developed to ensure continued availability of critical business functions in the event of a disaster or business disruption.



State of Nevada

Information Technology Security Committee

Policy

Control No.	Rev.	Title	Effective Date	Page
4.02	A	IT Security Policy	02/14/2002	3 of 4

- B. Departments shall appoint, in writing, one or more Information Security Officer(s) (ISO) dependent on the organizational structure, who shall be responsible for development, implementation, management, training and enforcement of policies and standards regarding the security of information technology.

6.0.2 IT Security Plan

- A. An IT Security Plan shall be developed for each agency at a minimum, with specific IT Security Plans for critical systems in compliance with this State IT Security Policy and requirements identified in associated State level IT Security Standards.
- B. IT Security Plans must be approved by the Department Head and reviewed by the State IT Security Committee as resources permit. The State IT Security Committee shall respond with comments and recommendations indicating whether the plan meets the minimum requirements of the State Security Policy and Standards. The IT Security Committee Chair will provide secure storage for the plans.
- C. IT Security Plans shall be developed based on the risks identified through a security risk analysis and the requirements for the specific IT processing environment.
- D. The IT Security Plan shall consist of specific policies, standards and procedures on the major security categories to include, but not limited to:
- Security Management
 - Security Awareness Training
 - Personnel Security
 - Data and Applications Security
 - Software Security
 - Communications Security
 - Physical Security and Environmental Controls
- E. The IT Security Plan shall be designed to respond to risks, threats and technology changes that may affect the department, the State or critical systems.
- F. IT Security Plans shall be reviewed and updated at least biennially or when major changes occur to the operating or physical environment, information technology and implementation of a major software application. The State IT Security Committee must review revised plans.
- G. Agency internal reviews of compliance to the IT Security Plan shall be conducted and documented at least annually.

7.0 DEFINITIONS:



State of Nevada
Information Technology Security Committee

Policy

Control No.	Rev.	Title	Effective Date	Page
4.02	A	IT Security Policy	02/14/2002	4 of 4

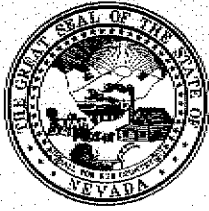
For the purpose of the I/T security policy and subsequent standards and guidelines, the definition and the use of the term "agency" shall be defined to be the department.

If the Department Director chooses to delegate I/T Security responsibilities to a division, bureau, board or commission, the term "agency", as used in these documents shall then be defined as applying to those organizational units.

8.0 EXCEPTIONS/OTHER ISSUES

Exception to the requirements of this IT Security Policy must be documented, provided to and approved by the IT Security Committee and the Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
State IT Security Committee Chair	Signature on File	02/14/2002
NV IT Operations Committee Chair	Signature on File	02/14/2002
Governor/Governor's Representative	Signature on File	06/17/2003
<i>Document History</i>		
Revision	Date	Change
A	02/14/02	Initial release.



Department of Information
Technology
Security



Standard

Control No.	Rev.	Title	Effective Date	Page
54:09	C	Wireless Network 802.11	01/30/05	1 of 4

1.0 PURPOSE

This standard provides for the basic security of IEEE standard 802.11 wireless devices and methods used to establish data connections.

2.0 SCOPE

This standard applies to DoIT and all state agencies that use DoIT for data connections for the deployment of wireless network equipment, to include access points, bridges, and their wireless clients.

3.0 EFFECTIVE DATES

The requirements of this procedure become effective immediately after sign-off by the DoIT Information Security Officer (ISO), Chief Information Security Officer (CISO) and Director or designee.

4.0 RESPONSIBILITIES

It is the responsibility of DoIT management and the DoIT ISO to ensure this procedure is implemented and enforced.

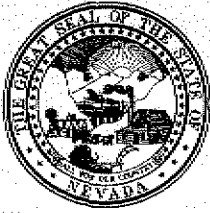
It is the DoIT Network Administrator(s) responsibility to ensure compliance with this standard and coordination with state agencies and security representatives to implement this standard.

5.0 RELATED DOCUMENTS/FORMS

State IT Security Standard, 4.02, IT Security Policy
State Data Communications and Remote Connections Standard, 4.62

6.0 STANDARD

- A. All wireless equipment will meet 802.11a, b or g standards.
- B. All wireless communications shall be encrypted.
- C. A separate authentication, authorization and accounting process must take place prior to allowing authorized wireless access points, bridges, or clients unrestricted access to nodes in an internal wired network. The authorization database cannot reside on the gateway between the wired and the wireless network and must reside within the wired network.
- D. Agencies shall conduct a site survey that will include, at a minimum, a detailed map of access point or bridge locations with expected service areas, channel assignments per functional area (if defined), documentation of street address and building name, floor and room location and system contact information.



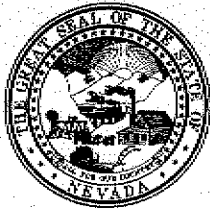
Department of Information
Technology
Security



Standard

Control No.	Rev.	Title	Effective Date	Page
54.09	C	Wireless Network 802.11	01/30/05	2 of 4

- E. Agencies must coordinate with residents of any adjacent structure within the signal coverage area to ensure radio interference does not occur.
- F. Default SSIDs shall never be used. SSIDs shall not be broadcast.
- G. Abuse, interference or disruption of authorized communications or unauthorized interception of WLAN traffic (see NRS 205.473 to 205.513), by use of sniffers or intrusion programs, is strictly forbidden. Authorized security staff is permitted to utilize these products and devices to audit and monitor their networks.
- H. Equipment must meet all applicable rules of regulatory agencies as established by both the Federal Communications Commission (FCC) and Public Utilities Commission (PUC). Vendor equipment is generally marked as certified for WiFi use.
- I. Dynamic addressing of nodes is not currently recommended for wireless networks.
- J. Whenever possible, access points and bridges shall be connected to protected ports on a Local Area Network (LAN) switch or router using port security based on MAC addressing.
- K. Wireless access points and clients shall be powered off when not in use. Wireless bridges should remain open at all times.
- L. Wireless access points and bridges must use secure administrative access methods.
- M. Wireless nodes or access points (not wireless bridges) that connect to the an internal data private internetwork, directly or indirectly, will be required to deploy to the following:
 - 1) 802.11i; or
 - 2) WPA; or
 - 3) IPSEC client VPN with extended authentication; or
 - 4) PKI with certificate solution.
- N. Agencies must document the following for use of wireless technologies:
 - 1) Benefits to the organization
 - 2) Who the intended users are
 - 3) How it will be used (applications or services)
- O. Wireless access points and bridges must be named as follows:



Department of Information
Technology
Security



Standard

Control No.	Rev.	Title	Effective Date	Page
54.09	C	Wireless Network 802.11	01/30/05	3 of 4

- 1) Budget Code, followed by;
- 2) Location Code – a whole number defined by the sysadmin, followed by,
- 3) Type of service code – a whole number defined by the system admin
- 4) Location code and service codes will be documented for reference.

7.0 EXCEPTIONS/OTHER ISSUES

The DoIT Director, CISO and DoIT ISO must approve all exceptions to this policy.

8.0 DEFINITIONS/BACKGROUND

802.11a – An IEEE specification for wireless networking in the 5GHz frequency range with a maximum 54Mbps data transfer rate. The 802.11a specification also includes Quality of Service (QoS) technology to protect voice and multimedia data.

802.11b – International standard networking technology for LAN wireless implementation that revised 802.11 to increase transmission speeds to 11Mbps.

802.11g – 802.11g will broaden 802.11b's data rates to 54Mbps within the 2.4 GHz band using Orthogonal frequency division multiplexing (OFDM).

802.11i – 802.11i is the IEEE standard for security in a wireless local area network.

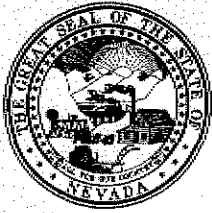
Access Point (AP) – Wireless LAN transmitter/receiver that acts as a connection between wireless clients and wired networks.

Internal (network) – a state administered network not available by default to the general public (Internet.)

PKI – Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.

SSID – Short for service set identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect.

VPN (Virtual Private Network) – A private data network that uses public telecommunications infrastructure while preserving privacy by using a tunneling protocol and other security measures. Using a VPN consists of encrypting information before sending it through the public network and then decrypting it at the other end. Companies have recently begun to consider using VPN to fulfill both their Intranet and Extranet needs.



Department of Information
Technology
Security



Standard

Control No.	Rev.	Title	Effective Date	Page
54.09	C	Wireless Network 802.11	01/30/05	4 of 4

Wireless – For the purpose of this standard, the IEEE 802.11x standards.

WPA (Wi-Fi Protected Access) – A specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi- Protected Access is derived from and will be forward compatible with the upcoming IEEE 802.11i standard.

<i>Approved By</i>		
Title	Signature	Date
DoIT Information Security Officer (ISO)	Signature on File	1/31/05
Chief Information Security Officer (CISO)	Signature on File	1/31/05
DoIT Director	Signature on File	2/23/05

<i>Document History</i>		
Revision	Date	Change
(A)	8/27/03	Initial Release
(B)	8/18/04	Total Revision of Wireless standards
(C)	1/30/05	Clarification of internal network

Billing

Electronic payments and payment by check must include the State's Document number, the billing claim number and the period of service (e.g. July, August, or September). Additionally, checks must be made out to (and sent to) the State of Nevada, Department of Information Technology, 400 W. King St. Suite 300, Carson City, Nevada, 89703-4204. Payments must be received by the State no later than the thirtieth (30th) day following the billed monthly.