Introduction
Government networks, given the nature of information they carry, demand the highest level of security measures. In addition, high availability and reliability performance requirements also top the list of every government wireless network bid specification. While many low cost wireless solution try to get their foot in the door, non have the ruggedness and reliability of Inscape Data SB3000 and BR3000 802.11n high capacity wireless solution.

Designed to thrive in extreme environments, the Inscape Data Corporation's SB3000 and BR3000 802.11n access and bridge solutions delivers rugged and secure wireless performance where it is needed, at the forefront of every secure network. With wireless 802.1x authentication, VLAN, access control list, advance encryption system (AES), and vandal & tamper resistant product design, government facility and staff will have access to high reliability, low maintain ace WLAN network on demand. With future proof design architecture, Inscape Data products can be up to date with firmware upgrade to the latest encryption algorithms to stay ahead of the pirates.

Government IT Trends
Several trends have developed those points to the need for pervasive wireless LAN in government facilities. With security and business continuity as a high priority on government IT list, mobility has emerged among the list.

Aside from healthcare professionals, government workers are one of the most mobile of all workforces. From maintenance personnel to transportation employees, thousands of government workers perform their jobs on the go every day. Wireless LAN becomes critical as a day to day tool to meet government objectives. Government entities cannot accept anything less than top level security in wireless access points and client devices.

Government policy
Government installations require top level security for very obvious reasons, to keep the government operating without unplanned interruptions. There are several requirements the government entity look for when purchasing equipments are:

- FIPS 140-2 Level 2 – This NIST developed standard specifies US Federal Government requirements for IT systems that are used for Sensitive But Unclassified (SBU) information. FIPS 140-2 specifies security requirements that must be met by a conforming product. Independent evaluators work with NIST and product vendors to validate a given product's security functionality. Since early WLAN security schemes (those based on Wired Equivalent Privacy, or WEP) were proven insecure, the only way government agencies have been able to deploy WLANs to date has been by utilizing a proprietary Layer 2 encryption mechanism. These proprietary encryption overlays are very expensive and complex and do not provide the mobility and radio-management benefits of centralized WLAN mobility controllers.

- DoD 8100.2 – This is the key DoD policy for the use of commercial wireless devices for non-classified communications within the DoD Global Information Grid. This policy requires that all DoD wireless infrastructure are both WPA2 certified and FIPS 140-2 certified for 802.11i. Such elements as layer 2 encryption, strong authentication, non-repudiation, personal identification, FIPS 140-2 compliance, addressing denial-of-service attacks, screening/sensing/monitoring, and other requirements are specified in this document.

- The Federal Information Security Management Act (FISMA) –FISMA requires all federal agencies "to develop, document, and implement an agency wide information security program". The National Institute of Standards and Technology (NIST) develop standards and provides guidance to federal agencies on information security practice. Their Wireless Network Security: 802.11, Bluetooth and Handheld Devices (Special Publication 800-48) is an excellent place to start in understanding the risks and possibilities inherent in wireless security.

- NIST approval of the IEEE 802.11i standard for WLAN security as acceptable for FIPS validation and impending approval of 802.11i by DoD for non-classified deployments. With availability of FIPS-validated 802.11i products, the Federal Government can deploy commercially available 802.1X authentication and layer 2 AES encryption for securing their WLAN infrastructure.

- Common Criteria – This is an internationally-adopted standard for information security. The creation of CC was lead by National Information Assurance Partnership (NIAP) program at NIST. Unlike FIPS, which provides a list of security requirements, Common Criteria provides a framework. Developers create their framework (referred to as a Security Target) and NIAP approved evaluators validate that a given product meets the claimed security functionality. When a particular framework for a class of product is widely accepted and approved by the NSA (National Security Agency), it is referred to as a Protection Profile (PP). In the Federal Government, Common Criteria validation is rapidly gaining acceptance as a key requirement.

Guest Services

Along with a list of stringent measures, the government IT staff need to extended connectivity services to guest due to daily influx of vendors, system integrators, visiting employees, and constituents within the building. Enabling easy access to the Internet for all can enhance productivity and efficiency. Guest internet access helps the vendors to have access to more information needed therefore providing better information for government staff to make better decisions. Wireless equipment with multiple SSID & VLAN is crucial in completing the guest services wireless LAN offering when paired correctly with the backend network systems.

Voice Services

VoIP is gaining ground as the go to method to deliver voice communications within the government organizations. By delivering voice and data over a single converged IP network,

acquisition and operational costs are significantly decreased. Additional benefits include lower costs for moves, additions and changes and increased productivity through presence technology that enables employees to reach each other on the first try. When voice over IP is deployed over wireless LANs, these same benefits are multiplied by making mobile workers reachable when they are away from their desks. Unlike cellular phone, service which may be spotty or nonexistent within a campus, voice over wireless LAN (VoWLAN) provides continuous, high-quality service when a secured wireless LAN is deployed.

Government facilities and organizations can realize many benefits from deploying VoWLAN services. One most important benefit is integration with existing voice services within the organization. Many mobile workers have resorted to using cell phones as their primary work phones. However, relying on cell phones precludes integration with the enterprise PBX, which may provide unified messaging, including a single voice mailbox, directory services, multiparty conference calling, and collaboration. When employees use cell phones, IT managers also lose visibility into the phone service; this, in turn, hampers support and makes it more difficult to assess telecommunications costs. What's more, many people work in jobs in which it's important that they be instantly accessible, no matter what their physical location. Examples include forensic technicians who need to be easily reached anywhere within the lab by prosecutors and detectives; and judges, district attorneys, and other officers of the court, who need to be reached anywhere within the court buildings.

Conclusion

A robust and scalable multi-service wireless LAN deployment enables new services that can significantly improve state and local government effectiveness both internally and externally. Deploying the Inscape Data Corporation’s wireless solution across a government organization enables comprehensive guest, security, and voice services. Through a robust and scalable guest network, vendors, system integrators and citizens can interact and make decisions on site, or simply make use of what was formerly unproductive time, imbuing government with a new sense of efficiency and service. Guest access also creates new ways for citizens to quickly request services or resources through Web portals and Wi-Fi-enabled devices, including smart phones.

Security services are a critical piece of any government IT security strategy to protect against wireless threats such as rogue access points. Immediate identification and prevention of such threats is critical in today's wireless age to maintain network and data integrity. As government organizations are likely holders of confidential citizen information, it is imperative that this potential vulnerability be fixed before the public's trust is violated as a result of a security breach. Voice services complete the mobile capabilities of government organizations by reducing inefficiency and the public's dissatisfaction with having to play voicemail tag. Cellular coverage does not have to be relied on within buildings. Even more important, advanced capabilities, such as presence technology, ensure that the right communication reaches the right person the first time.