One Page capabilities for submission to ATI for the Border Security Technology Consortium

Artel's greatest strength lies in the engineering, systems design, and life-cycle support of information technology (IT), communications systems, and information assurance. Since 1986, Artel, LLC (Artel) has evolved from an IT services company to a commercial satellite communications services provider and terrestrial circuits solutions developer to an end-to-end communications and cyber security systems integrator. Today, Artel delivers a full portfolio of satellite and terrestrial network communications and infrastructure, cyber security, risk management, and technology support services. Artel is hardware, software, and systems agnostic, tailoring solutions to fit customers' specific requirements.

Our experience managing the largest contiguous global terrestrial network in Africa has provided a continuous stream of knowledge and understanding of the delivery of strict Service Level Agreements (SLAs) in hostile and austere environments. This knowledge can be directly applied to the Border Security Technology Consortium. Artel is the largest provider of COMSATCOM bandwidth to the Department of Defense, providing C, X, Ku, and Ka band spectrum for mission-critical, diplomatic Intelligence Community and emergency response requirements. We provide higher service levels and enhanced backhaul services through our multi-protocol line switching (MPLS) fiber network infrastructure and ensure service continuity through our 24x7x365 Network Operations and Security Center (NOSC) located at our headquarters in Herndon, Virginia.

In direct correlation to the Border Security Technology Consortium, Artel has established a series of five scenarios in which communications solutions will be critical. We are developing multiple solutions for each scenario. The major parameters for each solution are speed, efficiency, mobility, and cost effectiveness. Several of our models are constructed for pay-as-you-go implementation:

1. Natural weather disaster – landlines and cellular are down for weeks, enabling minimal communications. Requirements: immediate local, regional, and long-distance communications.

2. Other natural disaster (e.g., earthquake, tsunami, volcano) – landlines down, cellular is spotty, power is minimal. Cellular for all communications could be the quickest to return but is power-grid dependent.

3. Terrorist attack – regional disruption with non-nuclear explosives at power stations, law enforcement, communications and data center hubs. Damage assessments could take months, restoration of communications additional months.

4. Terrorist attack – larger regional Electromagnetic Pulse (EMP) disruption. Anything with a chip is fried within a 100-200-mile blast radius at 30,000 feet and 200+ mile radius at 50,000 feet. No residual damage after the initial blast.

5. Terrorist or States-sponsored nuclear attack – authorities will have to deal with blast damage, radioactive fallout or seeding, and associated EMP. Initial requirements within the blast radius will be minimal. Most comms requirements will be at the edge of the blast radius.

It is our opinion that many of the solutions developed for these scenarios would be beneficial in protecting our borders. We also believe that the ATI stated areas of focus—surveillance and monitoring, identification and assessment, targeting and intelligence, apprehension/detention/seizure/removal—all require quick, efficient, and cost-effective communications and information management.