Prepared Statement of J. Alexander Philp, Ph.D.
President and Chief Executive Officer
GCS Holdings, Inc.
July 2, 2008

Thank you for this opportunity to testify before the Committee at this field hearing titled "Securing the Northern Border: Views from the Front Lines". On behalf of the citizens of Montana and the United States, I consider it any honor and privilege to come before you today and share my experiences regarding the challenges in developing a relationship with the Department of Homeland Security and drawing attention to technologies that have homeland security applications. I hope my testimony assists the committee in improving processes. I offer my testimony in good faith and acknowledge both the very real threats facing our nation's national security and the complex organizational, technological, and political challenges facing the Department of Homeland Security. I don't claim to be an expert on DHS-related policy or programs, but I have been actively involved as a Montana-based small business owner in trying to bring practical technological solutions to the front lines of Northern Border security.

Prior to the terrorist attacks on September 11, 2001, and the subsequent formation of the Department of Homeland Security, I worked and lived in proximity to the US – Canadian Border in Montana while serving as a National Park Service Ranger in Glacier National Park and later with the United States Forest Service, Lewis and Clark National Forest, living and working on the Rocky Mountain Front.

As I worked in these capacities, many of us were aware of common threats impacting the national security interests of the United States. Narcotics were flowing through Glacier National Park given its extremely remote and open border, small aircraft were landing at remote, unattended airstrips on national forest lands, enabling international drug trafficking, and clandestine trail and road networks across the border represented significant conduits for associated illegal activity.

My federal land management agency law enforcement colleagues did their best to bring attention to these issues and combat the problem. Nonetheless, very little was or could be done given the limited resources, antiquated technologies, jurisdictional conflicts, inadequate data sharing among local, state, and federal law enforcement agencies, and a host of other barriers to effective border security, especially in the more remote and rugged areas of the Northern Border shared between Montana and Canada. Moreover, especially in Glacier National Park, border and port security was an issue largely deferred to US Customs and/or US Border Patrol.

9/11 changed everything, and yet many and more of the security threats mentioned above remain effectively unresolved to this day.

In early 2002, I left the University of Montana – Missoula to form a company specializing in Geographic Information Systems, remote sensing, and development of applications to allows users to gain access to detailed geographical information. The company was based upon years of university research and development into next-generation technologies that enhanced the ability to interact with detailed geographical information about virtually any part of the world. The convergence of an

accessible internet, standardization in software, increasingly affordable and accurate data from satellite and ground-based sensor systems became the overarching thrust of our business plan.

Within months after the terrorist attacks on the United States, I was asked to serve on the Montana Governor's Homeland Security Task Force GIS Subcommittee and the Science and Technology Subcommittee. It is at this point that I began to experience what would become a long and inexplicable series of challenges in securing our nation's Northern Border. I have chosen to highlight a few of these experiences as a small business owner located in Montana, and provide my perspective on the disconnects. I will summarize my critiques.

As I mentioned, my service on the Homeland Security Task Force Geographic Information Systems (GIS) subcommittee revealed a number of interesting realities. For many members of the committee, primarily local, state, and federal government, subsequent DHS-related funding activities post-9-11 resulted in a wind-fall for spending ranging from everything from HAZMAT suits, to software and hardware purchases, to data purchases, to various failed programs and projects. We failed to work the problem from a vulnerability perspective, assuming equality to terrorist threat vs. looking at what elements of Montana were the most vulnerable from a counterterrorism and counterintelligence perspective, and how Montana could be utilized by our enemies as an easy-entry point, "soft-underbelly" to our nation's borders. We failed to look at the problem holistically.

While the work of the committee was attempting to address homeland security related issues, we were, in essence, disconnected from DHS core missions, regressing into existing state-centric GIS activities. While I was unable to attend every meeting, virtually no attention was placed on the security issues associated with the Northern Border while a great deal of time, energy and money addressed data standards, critical infrastructure identification and localized threat and risk assessment, and some effort on how to share and comingle rich localized spatial data resources with top-down, federal programs emerging out of DHS with the support of the National Geospatial Intelligence Agency (DHS).

In hindsight, given the significant security issues facing the Northern Border and transnational energy security, i.e., pipelines, power lines, and future energy security issues, the GIS Subcommittee should have focused more attention and resources on addressing these issues. Eventually, the funding bonanza came to a close. Issues of local, state, and federal data sharing, prioritized risk against threat, examining Montana's geopolitical posture within the content of the global war on terror (GWOT) and a more effective working relationship with DHS federal agencies responsible for homeland security remain outstanding issues.

As a final observation, it was also clear that there was a great deal of resistance by some members of the committee to issues associated with security clearances and national security policy in general. Connecting local Montanans with a sense of urgency regarding national security *vis a vis* Montana-Canadian border was virtually impossible based upon my observations. We were too disconnected in many respects for the real challenges and hard work of local, state, and federal civilian law enforcement and DHS in general.

Regarding the Science and Technology Subcommittee, I attended one meeting and suggested that attention be placed on cyber, chemical, biological, radiological threats, in particular potential attacks on food and water resources, and SCADA control system attacks on the power grid, and these

comments fell on deaf ears. The committee may have met once or twice again, but due to lack of effective leadership, I believe it was defunct a short time after its creation.

As a second example, based upon previous work at the University of Montana, and interaction with the US Intelligence Community and Department of Defense organizations, my company was contacted by the US Navy, Naval Undersea Warfare Center (2003), regarding an opportunity to license and transfer sensor technology recently declassified by the Navy.

The technology was specifically developed to address issues associated with covert and clandestine monitoring of perimeters, borders, and critical infrastructure. The sensor system technology relied about buried a fiber optic cable that could detect, track, and classify targets as they passed over or in proximity to the buried fiber optic cable. Armed with a declassified technology brief supplied by the Navy, I requested from the US Attorney Office in Montana a closed-door brief on the technology and capability at the Transborder Terrorism Conference held in Whitefish, Montana (2004). Approximately, 40 individuals attended the brief.

I presented the declassified information on the sensor system (code-named BLUE ROSE), as a potential candidate for intelligence and surveillance activities along the Montana-Canadian border. I spoke with individuals from the International Boundary Commission, Royal Canadian Mounted Policy (RCMP), and many others. Following the presentation, I was approached by a Customs and Border Protection (CBP) official who expressed interest in learning more.

Following the conference, I supplied detailed information, pricing estimates, and integration techniques with commercial GIS, remote sensing, and associated value-add to the BLUE ROSE sensor system. I worked to coordinate information exchange between the US Navy, my company and DHS CBP. I was asked to present to local and sector CBP, Border Patrol (BP), and Immigration and Customs Enforcement (ICE) agents and develop a CONOPS – Concept of Operations for a BLUE ROSE 3CIS implementation along the US-Canadian border, which I did.

Eventually, the information, costing, CONOPS, and scope was internalized by CBP and BP into an internal governmental request for a pilot project to test, evaluate, and demonstrate the capability of a multi-million dollar advanced prototype system developed and licensed from the US Navy for a specific area of interest (AOI) along the Northern Border. As the pilot program concept and technology was internalized by DHS field staff and submitted up the chain of command, it became difficult to track the progress of the proposal and opportunity. However, this was to be expected since I clearly did not have access to these internal DHS conversations nor were we ever invited to discuss the merits of the program following our detailed disclosures and costing estimates provided to those CBP and BP agents who wanted a pilot program. We also were aware that as a small business we were facing some herculean obstacles in ever having a real-program funded.

However, we felt that half the battle was achieved in that we did the work of bringing the technology to the attention of the responsible parties, briefed them on capability, notified all parties of progress, and had worked to substantially reduce the costs of a well-conceived, prudent, and timely pilot project, upwelling front from the front lines of the border security reality. Months passed as we waited to hear on the outcome of a year of effort to bring this capability to the attention of DHS HQ.

Ultimately, it was rejected, and to this day, I am personally unclear of the reasons for the rejection, although I can share what I heard through my contacts. At the time, America's Shield Initiative (ASI) was the Holy Grail, one-size fits all solution for securing our nation's massive borders, and the government request was viewed as duplicative – "everything will be handled by ASI". Secondly, bottom-up proposals from folks on the ground, fighting the fight, don't get very far up the chain of command. If the idea does not originate in Washington, D.C., the likelihood of implementation is low to none, unless you have enough political power to dialogue directly with the DHS-based decision-makers.

Existing bureaucratic battles between "the guys in green" and "the guys in blue" under the umbrella of the newly formed DHS impacted the likelihood of proposal success, especially given that port security and the land in between the ports are managed by two different groups - green and blue.

Subsequently, my company watched in disbelief as subsequent SBIR topics, Broad Agency Announcements, and other DHS solicitations appeared calling for the very capability represented in the BLUE ROSE technology. This occurred on a regular basis well into 2005-2006, until such a time as ASI was over and a new program was conceived: Strategic Border Initiative (SBI) and (SBI-NET).

As is typically the case, and certainly the *modis operandi* with DHS, SBI was going to be a big, multi-billion dollar program. Vendor days were held in D.C., making it extremely difficult from my business to attend. Large defense contractors were encouraged to build mega-proposals and solicit small-business innovation as part of their major teams. Eventually, as a result of our license of the BLUE ROSE technology, most of the major US Defense Primes did make their way to Missoula and inquired about our capability. This usually meant a team of four or five gentleman who cannot understand what they are doing in Montana outside of a ski vacation or buying a vacation home while they conducted due diligence on a world-class, next-generation technology as part of the overall proposal to DHS for SBI.NET. Eventually, my company was included on the team represented by one of the four major companies that offered up proposals to DHS. BLUE ROSE and other capabilities of our firm were included, but unfortunately, our team prime was not chosen, and BLUE ROSE was buried again.

In order to survive during this long-term commercialization effort, our company eventually partnered with the Department of Energy, Idaho National Laboratory and focused our attention on multi-dimensional protection of critical infrastructure as opposed to trying to get the attention of DHS and/or successfully partnering with a major defense prime regarding the effective deployment of this capability in select areas of interest.

In addition to what I stated above, I learned a great deal about the difficulties in successfully developing a relationship with DHS at the levels necessary to effect change. First and foremost, small business is inherently at a disadvantage every step of the way. Most major projects are controlled and run by nation's largest defense contractors. Unless you have a long-standing relationship with them, they aren't interested. Secondly, as a small business, it is absolutely critical that you have a presence in the Washington, D.C. beltway. You can build relationships all day long in the field, on the front lines, but unless you are on the radar in D.C., things aren't going to happen.

All the major decisions, personalities, and decision-makers are there. We used to think that if you had great, innovative technologies that could be included and integrated into an overarching solution that met the needs of the agents on the ground at an affordable price, then somehow these

capabilities and opportunities would surface. I no longer think this way. I take responsibility for my naiveté and idealism.

Despite our best attempts given our limited resources as a small business, the barriers are just too numerous to success. Providing American's and Montana's with cost-effective, elegant technologies to address the multi-faceted threats facing our nations became a mirage.

The barriers fall into four major categories: the contracting process as a legacy of contracting officer understaffing at DHS, DHS top-down, big-business contracting tendencies, bureaucratic turf battles among the previously independent agencies, and a politically-motivated chain of command.

My final example falls into a related category. Having worked as a Park Ranger in Glacier National Park and GIS technician for the US Forest Service, I was sensitive to the challenges associated with law enforcement of the vast western public domain.

Beginning in 2006, I was contacted by a colleague who serves as a Law Enforcement Officer (LEO) for the United States Forest Service. He stated that other colleagues of his were desperately attempting to find reliable, accurate, and up-to-date data sources for portion of the US-Canadian border that showed clandestine trail networks, i.e., ATV tracks, hiking trails, transborder logging roads, etc. Prior to 9-11, the USFS was often leading the way in sensitive law enforcement activity associated with this type of border insecurity and the associated illegal activity.

Upon this request, I met with key personnel with the USFS LEO community and discussed their needs as well as the dynamics of their participation in one of the regional Integrated Border Enforcement Teams (IBETs), comprising, multiple DHS agencies, USFS, RCMP, and other federal jurisdictions concerned with securing the Northern Border.

At the request of the USFS, as well as the Rocky Mountain Information Network (RMIN), a US Department of Justice funded Law Enforcement data resources network heavily used by members of the law enforcement community, I examined the existing GIS data condition and resources.

At the time, key LEOs were utilizing a paper map hanging on a wall with poorly documented data, misalignment, improper projections and scale, and no reliable US-Canadian data resource for vector feature (line features) alignment. I was further surprised to learn that the key paper map had taken an incredibly long time to produce and cost the taxpayers an unbelievable sum, approximately 10x what a decent GIS company would charge. Most importantly, the resource was paper, not digital, and did not support the field operatives in terms of mobility, usability, GPS-interoperability, or reliability. We had a 19th century solution to a 21st century problem.

Many were already relying upon the early version of Google Earth for their core geospatial intelligence (GEOINT), but did not realize that the data in Google at the time was outdated and relied upon the wrong data sources to adequately provide them the road and trail networks they needed. Moreover, given the sensitivity of their positions, and the incredibly dangerous and isolated nature of their work, many of the USFS LEOs were hesitant to rely upon other USFS GIS technicians for assistance given the lack of operational security. Trust plays a key role in law enforcement activity given the fact one's life depends upon it.

My company eventually provided a cost and technical proposal to the USFS representative to the IBET. Unfortunately, my primary point of contact who had requested the proposal was transferred to a new area and the champion of the innovation was no longer available. Despite this, I was requested to provide a non-classified briefing to the IBET near Spokane, Washington to discuss the proposal, examine the problem, detail the nature of the geographical information available to them, and the merits of yet another pilot program. Moreover, RMIN was so supportive and the cost proposal so affordable that they were willing to cover the costs of the pilot as long as a member of the IBET requested the implementation of the "BorderView Program," as our proposal was entitled. Again, so close, yet so far.

During my briefing, I found an audience that was generally woefully unprepared to learn about the realities of these technologies contained in my proposal and sincerely believed that a "magic bullet" was coming from DHS HQ soon that would address all the problems outlined in the needs-assessment meeting with the USFS LEO. Certain members, having recently seen a press release put out by a large GIS vendor and DHS, actually believed that when the software arrived it was be the same as the solution I had proposed. They told me that the satellite imagery I was to provide was available on Google, etc. Other members of the IBET saw merit, but in typical group think felt that if there was opposition from some elements based upon "lack of need" then it was better not to rock the boat. Folks in federal agencies normally do not normally like to stick the necks out, and for good reason. Of course, I was asked to leave following my presentation, so classified discussion could occur. Following the conclusion of the meeting, I was told they liked it very much, learned a great deal, and they would get back to me.

Eventually, I learned that the USFS Region 1 LEO authority did not want to take the political risk of requesting the funding from RMIN for the project to proceed, and the yearlong effort came to a close. To this day, many of the needs expressed by the original USFS LEO are not met. However, hundreds of millions of dollars have been spent attempting to deliver an overly complicated system that fails to meet the day-to-day, in the field realities of the men and woman on the fronts of lines of securing our nation's borders. There is something very wrong with this pattern.

Furthermore, no "magic bullet" ever arrived in a box from DC to meet the original goals and objectives of the program. In the absence of an organized, integrated solution, I continue to support my friends who need assistance if and when needed and I do this work gratis since it is impossible for my firm to contract successfully with the USFS and other federal civilian land management agencies given the dominance of large firms that own the multi-year contracts or firms that serve as embedded contractors with the agencies. In my opinion, this example underscores a number of radical disconnects, extreme waste of taxpayers' resources and, most importantly, the chronic and persistent inability to meet the information and technology challenges in a timely, cost-effective manner.

Unfortunately, I could continue, but I chose to highlight a few examples of the multifaceted difficulties my company has experienced in attempting to develop a relationship with DHS and bring technical solutions to bare on particular elements of homeland security challenges. The unique challenges along the Northern Border are defined geographically, topographically, economically, meteorologically and culturally. The national security challenges endemic to the massive Northern Border, including Montana's 545 miles of shared border with Canada, require a significant shift toward a bottom-up – top-down balance.

The national security challenges require the rapid harvesting of innovative ideas and solutions that present significantly more cost-effective, localized application. They require the ability to never lose site of the field officer and the prime directive that the technologies be successfully integrated to the point that the field agent can successfully utilize the tools in his or her day to day operations. The technologies need to be integrated into a unified, standards-based, highly-interoperable, flexible architectural framework that can change cost-effectively to meet the local and regional security challenges facing the field agents, in particular those who are on the ground in some of the most extreme and remote environments imaginable – outside of Alaska.

The technologies must never been seen as anything more than tools in an evolving toolkit designed expressly to the greatest common needs identified in the field. My continued hope is that we can work together to solve the complex and unique security challenges facing the Northern Border, utilizing in a cost-effective manner the right technologies at the right times in the right places and provide practical, incremental improvements in how field agents conduct operations on a day-to-day basis.

I would be happy to answer any additional questions the Committee may have and discuss ideas I have regarding improving the overall process. Thank you for attention to this matter and for the opportunity to appear before you today.