



BLACKHAWK
Management Corporation

Central Region

INFORMATION TECHNOLOGY

WHITE PAPER

04/07/06

*3535 Piedras Drive West, Ste 100
San Antonio, Texas 78228
Tel (210) 736 645-5420 • Fax (210) 736-5370
Email: witherowl@blackhawkmgmt.com*



Table of Contents

Section	Title	Page
1.0	Introduction	3
2.0	Information Technology Planning	3
3.0	Information Technology Technical Support	4
4.0	Network Management (Classified and Unclassified)	4
5.0	Network Administration	5
6.0	Systems Administration/Data Management	5
7.0	Configuration Management	6
8.0	Storage Management	6
9.0	Information Assurance	7
10.0	Intrusion Detection	7
11.0	Disaster Recovery/Continuity of Operations Planning	7
12.0	Training & Help Desk	8
13.0	Help Desk Support	9
14.0	VTC Design	9
15.0	Software Life Cycle Management	10
16.0	Software Development	11
17.0	Enterprise Management Systems (EMS)	11
18.0	WEB Support	12

1.0

**Introduction**

BLACKHAWK has a 15-year history of providing Information Technology (IT) services ranging from IT Planning, Deployment, Operations, and Maintenance to Help Desk support. We provide these services to the Department of Defense (DoD) and federal agencies, as both the prime and as subcontractors to other large Defense Contractors. BLACKHAWK continually researches and incorporates new technologies and best practices into our IT processes and provides on-going education to our engineers. In this manner, we achieve continual improvement of our services and products and maintain a high level of customer satisfaction.

The following sections provide brief descriptions of our inclusive range of IT services with samples of relevant experience.

2.0 Information Technology Planning

BLACKHAWK provides customer solutions for technology challenges that are faced in common every day support environments and unique austere contingency environments. We support integrated applications, services, and network transport capabilities across war fighting, intelligence and business mission areas that enable leader-centric operations anytime, anywhere, at every echelon. Our planners have designed and employed large scale services deployments in both tactical wartime environments, and in fixed or sustained business environments. We successfully developed and maintain a 5-year plan for the Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS) that increases network capability and reliability, and meets future command and control requirements for the US Army units at Ft. Hood.

We plan and assist with the implementation of current and future services which include Active Directory, Microsoft Exchange, Portal and Document Management, Cisco WAN, LAN, and wireless networking that the US Army's III Corps and subordinate divisions and separate brigades use. Included are deployment and support in Operation Iraqi Freedom, MILLENNIUM CHALLENGE, Mission Rehearsal Exercises (MRX), ULCHI FOCUS LENS (UFL) and Command and Control (C2) communications testing exercises.

BLACKHAWK tracks technology trends, which then drives our research and training activities. We make sure that our technology team is continually aware of technology changes and trained accordingly. Therefore, we are able to use a wide variety of resources to ensure that we create the best implementation plan for projects. We also encourage members of our teams to continue their professional education and seek industry certifications through company supplied resources, vendor training, and local colleges.

By attending Information Technology (IT) conferences and vendor demonstrations, and reviewing trade magazines our network planners maintain knowledge of the latest technology trends, methods of integrating these technologies into the work environment, and procedures that improve the overall efficiency and effectiveness of the network. In addition, we maintain good working relationships with vendors to ensure that we always have the technical support we need with their products.

BLACKHAWK also maintains access to technology experts through a well-established relationship with the University of Texas, San Antonio, Center for Infrastructure Assurance and Security (CIAS). This organization of industry and academia is certified by the National Security Agency (NSA) and is establishing a reputation within the Homeland SECURITY Community. We

**Management Corporation**

use their in-depth knowledge of technology trends and advancements to aide in reducing risks to our customers when we respond to new, ever changing mission requirements, business process re-engineering challenges, and emerging threats to war fighter information operations and their supporting net centric IT environment.

3.0 Information Technology Technical Support

BLACKHAWK has been successful in staffing highly skilled IT professionals for our customers who experience resource shortages and variations due to either high turnover or reduction in civilian employees. We provide 15 engineers to the US Army HQ III Corps elements who function as Information Management Officers/Information Assurance Security Officers (IMOs/IASOs). They perform a variety of IT functions, including day-to-day administration of all Microsoft® products, computer related hardware and peripherals, including printers. Our engineers maintain all hardware and Hardware Lifecycle Management program accountability. We track and monitor systems over their life span and enable the government to accomplish a complete technology refresh every 4 years.

BLACKHAWK utilizes imaging software to maintain the latest standard configuration and ensure that system upgrades or reloads take a minimum amount of customer's time. Our engineers stand ready at all times to immediately respond to all critical trouble tickets and effect restoration within 2 hours, during duty hours. After duty hours we respond within 2 hours and effect restoration within 4 hours. BLACKHAWK follows guidelines to ensure that all software is licensed and ordered through the proper channels and advises on all hardware purchases as required by the government.

Our expertise is applied across the US Army's Ft. Hood as requirements for IMOs and IASOs increase. BLACKHAWK anticipates that as mission requirements increase, so will the demand for BLACKHAWK's support.

4.0 Network Management (Classified and Unclassified)

BLACKHAWK provides highly skilled network engineers and system administrators for effective network management. Our engineers assist in streamlining and automating many mundane processes, such as router and switch management that consume engineers' valuable time. We use our skills and past network experience to suggest and implement time saving, automated, and secure solutions to permit a proactive, rather than reactive, network environment.

For the US Army at Ft Hood we manage and maintain both unclassified and classified networks that have more than 10,000 users. BLACKHAWK engineers are able to keep pace with current technology and plan for future technology including technical aspects and business processes. Our practices ensure a responsive network that satisfies the unique needs of numerous customers. We provide a singular responsible element dedicated to network management, Information Assurance (IA), intrusion detection, configuration management, and network expansion.

For the Air Force Outreach Program Office (AFOPO) at Brooks City-Base, TX, BLACKHAWK manages and implements information systems that includes of a variety of network support. We assist with technical requirements, development, systems acquisition, implementation services, user assistance, help desk, and system support. The AFOPO network consists of more than 14 users arranged in LAN and WAN topologies at Brooks City-Base. A Network Operations Center (NOC) with an embedded help desk provides services for the network community.

**Management Corporation**

BLACKHAWK plans, designs, installs, and troubleshoots the entire information technology network architecture and maintains computer security and integrity within AF Computer Emergency Response Team (AFCERT) guidance. Our engineers maintain the Microsoft Server 2000/2003 Active Directory network; monitor ongoing network system operations; ensure that the hardware and software are functioning properly and that operational standards are met; and identify and correct security vulnerabilities in accordance with AF guidance.

5.0 Network Administration

BLACKHAWK uses our extensive network knowledge and experience in managing both classified and unclassified network devices to provide quality services for many DoD organizations. We understand the similar services each provides and the key differences and risks associated their operations. Our engineers are adept in managing both types of networks and mitigating their different security risks.

We deploy innovative measures to protect the networks from Internet intruders, inside user negligence, and configuration errors that could cause system compromise. Our engineers monitor and enforce appropriate procedures for physical security such as password management, position of terminals with respect to doors and windows, removable data storage hardware, and static protection for hardware devices stored in safes. For both environments BLACKHAWK manages the IP addressing schema to ensure proper segregation and allocation of IP addresses.

BLACKHAWK avoids service interruptions by spending dedicated time in tracking network performance baselines and ensuring deviations are properly tracked and monitored. Included in our baseline configuration is the tracking of IP addresses as they are issued, revoked, or changed.

At Lackland AFB, BLACKHAWK provides training, installation, configuration, documentation and operational support for the 690th Intelligence Support Squadron networks. These networks consist of more than 3,000 users with accounts on three separate networks: NIPRNet, SIPRNet, and JWICS. It includes 300+ network printers at various locations across the Air Intelligence Agency (AIA) complex at Lackland AFB including the agency headquarters and subordinate units, the Air Force Information Warfare Center, the Air Force Cryptologic Support Group, the Joint Information Operations Center KellyUSA (formerly San Antonio Air Material Depot) and Lackland Training Annex.

6.0 Systems Administration/Data Management

BLACKHAWK provides services and tools that comprise an enterprise architecture roadmap for defining and implementing an effective business system to support the full range of IT functions. We work from the premises that network dependability, data integrity, and reliability are critical to the success of supported networks; that constant monitoring of network performance, productivity, and validation and verification of data are essential. BLACKHAWK follows a process for careful monitoring of networks and variances and quickly taking corrective actions in achieving network dependability, data integrity, and reliability. We have proven experience in the IT planning, development of operational requirements, and engineering of both mission critical IT service solutions and command and control network infrastructures.

Our Engineers migrated the US Army III Corps and Ft. Hood JWICS and SIPRNet Domains from NT 4.0 to Windows 2003 Active Directory infrastructure without disruption to subscriber services and network resources. BLACKHAWK was recognized as the first in the Continental United States Army to successfully complete this migration. Our system engineers have proven

**Management Corporation**

experience and practice implementing and supporting Windows 2003 Active Directory technologies, including migration planning; infrastructure engineering and design; operational platform management and monitoring; software and group policy deployment strategies; production support; and system engineering.

BLACKHAWK engineers support the US Army enterprise network services both in fixed garrison environment and in a deployed area of operation (AOR). Our engineers provide DNS, WINS, DHCP, IIS, FTP, SUS, VOIP, exchange messaging, and mail security applications. These are deployed in a tiered architect solution which supports forward deployed forces, provide reach back capabilities, and allow information exchange for operational messaging capabilities between garrison and forward deployed forces.

7.0 Configuration Management

BLACKHAWK applies in-depth experience and proven capabilities for accomplishing Configuration Management (CM). When specified, we provide CM according to the CM practices of our respective customers. If a specific CM process is not specified by the customer, we follow our AS9100 Quality Management System (QMS) CM procedure. BLACKHAWK's CM procedure specifies the responsibilities and authorities for the CM process. It defines the requirements which we adhere to for configuration management planning, configuration identification, change control, configuration status accounting, and configuration audits.

BLACKHAWK is a contributing member of the US Army Ft. Hood Configuration Control Board (CCB). Our board members provide technical support, advice, and user feedback to the board. We understand the purpose and necessity of the CCB, and through our support we ensure that requirements are clear and quantifiable, and address changes and impacts. In our role, we make sure that proper coordination of changes occurs prior to their implementation.

BLACKHAWK helps the CCB manage the current and historical status for each change. We ensure that requests are properly documented and include the chain of approvals. We champion continual robust CCB meetings through which we aggressively control baselines, i.e., hardware, software, and documentation.

8.0 Storage Management

BLACKHAWK engineers provide numerous storage management solutions including Network Attached Storage (NAS) and Storage Area Network (SAN) deployment strategies that simplify enterprise storage management. We provide the foundation for storage consolidation, storage flexibility, high availability, and network storage growth capabilities. Our engineers possess proven experience in providing high data availability of operational critical data, controlling data resources, and responding to the on-demand enterprise storage requirements.

BLACKHAWK implemented a sound backup and recovery process after carefully analyzing the impact of lost data, frequency of data change, and database size. Our process requires us to assess each backup and recovery option with the value of the data and military impact as the primary drivers. These decision elements drive the frequency of backups and focus of the backups.

We currently administer a NAS in support of the SIPRNet subscriber domain that provides an efficient and reliable means of information distribution for the US Army III Corps and primary staff. BLACKHAWK engineers use their expertise in the deployment of software and hardware based technology to support recovery operations as well as Continuity of Operations Planning

**Management Corporation**

(COOP) and designs. We assist in providing a viable COOP strategy in support of response and recovery operations as well as continuance of critical network services.

9.0 Information Assurance (IA)

BLACKHAWK provides solutions to customers whose networks experience attempted intrusions and software viruses that threaten network security and mission accomplishment. We apply our comprehensive secure network experience and abilities to assure mission accomplishment on the US Army network at Ft. Hood. Our engineers maintain firewalls and intrusion detection devices that include the Cisco PIX, Sidewinder, ISS Real Secure, and other top industry devices. We create well-defined plans of comprehensive solutions and develop solutions to network intrusions that ensure secure operations.

BLACKHAWK provides technical leadership for one of the largest DoD developed Intrusion Detection Systems (IDS) in the US Army. Our engineers technically led the development from the ground up, of an IDS written in Java, Perl, and Shell working with an Oracle Database. This IDS provides oversight and protection to every unclassified Demilitarized Zone (DMZ) in the Air Force. The firewall configured database records more than one million connections an hour with on-line backup routines in place.

BLACKHAWK employs IA experts who are certified in both Harris Stat Scanner and eEye Retina. They identify current vulnerabilities on the network and remove them. Our engineers have led the identification process and repair action implementation for vulnerabilities at more than 20 Air Force Bases worldwide. For the US Army at Ft. Hood we use Windows 2003 Active Directory Group Policy Objects (GPO's) and Systems Update Servers (SUSs) that permit devices to receive patches with automated configuration download. We monitor the currency and effectiveness of these processes and tools on an ongoing basis.

A Defense Information Systems Agency (DISA) team reviewed the Ft. Hood Network which we manage and reported no IA Vulnerability Alert (IAVA) findings. They recognized Ft. Hood as the cleanest and best managed network they had visited.

10.0 Intrusion Detection

BLACKHAWK provides AI experts to successfully perform the complex tasks of protecting networks from intrusion. Our engineers hold the highest professional certifications in the industry and BLACKHAWK continually builds upon their skills with training on the latest technologies. In this manner BLACKHAWK makes the difference in providing intrusion detection and prevention on our customer's networks.

Our IA experts provide maximum security of the Directorate of Information Management (DOIM) network by applying new and proven technologies in a timely manner. We maintain security levels required to thwart various threats, and apply current threats and counter technologies that thwart sophisticated threats.

11.0 Disaster Recovery/Continuity of Operations Planning

BLACKHAWK applies disaster recovery experience and expertise in developing and maintaining disaster recovery plans, providing Continuity of Operations Planning (COOP), and performing contingency planning. With these plans we produce the implementation plan for courses of action (COA). We have successfully developed these plans for the US Army Ft. Hood DOIM and at other sites.

**Management Corporation**

BLACKHAWK's plans are a combination of the proven methods of our engineers and the best practices of industry and the US Army. We cover the width and breadth of operations in planning so that any type of disaster can be mitigated with the least operational impact.

Included in our planning is the provision of off-site storage options and alternate placement of key services that avoid extended service outages due to disaster or other anomaly and ensure continuity of operations. We develop Techniques, Tactics and Procedures (TTPs) that include decision planning prior to an incident, and ensure that we can make timely decisions with government leaders. BLACKHAWK's proactive approach to disaster recovery planning is key to providing a Network Operations Center with uninterrupted and reliable operations, and survivability of the services during a major disaster or contingency.

12.0 Training & Help Desk

BLACKHAWK provides training, installation, configuration, documentation and operational support for the 690th Intelligence Support Squadron's networks at Lackland AFB. These networks consist of over 3000 users with accounts on three separate networks, NIPRNET, SIPRNET, and TS and 200+ network printers.

We develop and teach hands-on computer hardware and network courses at the HQ/AIA that are tailored to our AIA customer's requirements and needs. Our instructor provides student workbooks, hands-on training, and concludes with an Initial Qualification Test (IQT). One course we teach is a two week Client Support Administrator (CSA) class. This course includes training on hardware, networks, software configuration and applications, and webpage development. Students are tested at the end of each section. At our CSA course conclusion, all CSAs must pass the IQT before they are given CSA permission and rights.

An important aspect of our training is Question and Answer (Q&A) sessions. These Q&A segments provide students with important answers to how the information presented is applied to the AIA networks.

During the hardware session of the class, we teach CSA students about the various hardware and firmware components of the personal computer. Our instructor leads a hands-on lab in which students tear-down and reassemble a working computer to reinforce what they have learned.

For the network session, we present the CSA students with a thorough review of various network components, related services (DHCP, DNS), and network architectures. We include definitions and discussions of IP address, subnets, computer cables and their applications.

CSA students are also taught how to load and configure Window XP Professional with other unit baseline software such as includes Microsoft Office, Outlook, Antivirus software and Internet Explorer. They are trained to load, configure and use NETIQ DRA, the main application used to give CSAs the ability to manage user and computer accounts. Our instructor frequently includes a session on webpage development. We show students how to use a simple text editor to develop a basic webpage.

Our systems implementation support includes installing, configuring, operating, and maintaining UNIX (Solaris) and Windows NT/WIN2K Professional on Workstations, clients, desktops, laptops, Enterprise Servers and Windows 2000 in a cluster server environment. We Install, configure, operate and maintain UNIX and windows-based applications on clients and servers, such as Microsoft Enterprise BackOffice products: Microsoft Exchange, System Management Server, SQL Server, Internet Information Server, NT Server, and Windows 2000. Our engineers troubleshoot,

**Management Corporation**

isolate, and correct problems/anomalies encountered in the installation and use of UNIX and Windows NT Workstation, UNIX and NT Enterprise Server, Windows 2000 products, and Microsoft Cluster Server.

We provide system integration support which includes Work Group Manager, System Administrator, Network Administrator and helpdesk administrator training in PC fundamentals (system configuration, troubleshooting, teardown and rebuild of PC), Network Essentials (protocols, architecture, topology, IP addressing and hardware), Windows 2000 (installation and configuration) and Website design (HTML). Administrator training includes workstation installation, configuration as a server/client, customizing user environment, installing/configuring routers and switches

Our engineers perform Help Desk functions such as troubleshooting and installation support of computer resources for 3,000+ users on three networks; support and installation of Windows 2000 Professional, Office 2000 Professional, Norton AntiVirus, FormFlow, WinZip, Acrobat Reader, Security Banner. Other tasks include developing transition plans describing actions and resources required; providing monthly network availability and reliability statistics of network servers and devices; providing statistical analysis showing performance degradation /improvements; and, providing historical analysis and trends.

13.0 Help Desk Support

BLACKHAWK uses our understanding of Help Desk Support operations and our capability of being responsive to resolve technical issues within specified customer timelines. We work proactively with customers in requirements definition and planning for network support. As the number of network users increases we plan with the customer and add needed resources to address the resulting increase in network requirements.

BLACKHAWK maintains processes, procedures, and standards for their work with the US Army III Corps. We developed and utilize a help desk suite to track trouble tickets in the III Corps Headquarters. This enables us to provide more efficient and effective mutual support and ensure the mission is accomplished, as well as information sharing to avoid duplication-of-effort.

In addition to trouble tickets, our team maintains user account requests. We employ naming standards per our customer policy. We integrated these into the Help Desk function to facilitate business proficiency.

14.0 VTC Design

BLACKHAWK provides total planning, acquisition, installation, and operational support to the AFOPO in acquiring, deploying, and maintaining their Video Teleconferencing (VTC) Capability. We first perform an assessment of the user's needs and obtain an agreement by our customer on the design and planned implementation. We proceed through design, development and implementation with customer reviews and installation of the VTC that meets the customer requirements and needs.

Our engineers design and install systems that range from small, self-contained portable units (just out of the box) up to complete auditorium integrated VTC capabilities. In providing the complete auditorium integrated VTC capabilities, BLACKHAWK installs all the associated VTC equipment. This includes mounting speakers in ceilings, hanging microphones from ceiling over conference room tables or seats, mounting the camera(s) on the walls, integrating in "whiteboards", integrating in presentation capabilities (through a presentation camera system...the VTC equivalent to a view

**Management Corporation**

graph machine), and installing an integrated controlling device for single point-of-control and remote control of all the components.

BLACKHAWK tests and verifies VTC systems, and provides user training and operational assistance to AFOPO personnel as necessary. We coordinate and plan all VTC connections which include remote site capability, compatibility, and availability to support scheduled VTC sessions. Our engineers not only support the AFOPO in their VTC capabilities, but have become the troubleshooting experts at maintaining the Secretary of the Air Force Small Business Office's (SAF/SB's) VTC capability. We are repeatedly requested to bring SAF/SB's VTC capability back on-line, and in all cases BLACKHAWK has accomplished that task on-line (phone and VTC) without leaving Texas!

BLACKHAWK has been designing and implementing VTC capabilities at various locations for various customers since 1997. We are technically knowledgeable in all aspects of current VTC systems and their capabilities. Our engineers ensure that their systems not only function at their maximum capability, but that those systems are in compliance with all current DoD security directives. Furthermore, BLACKHAWK ensures that their systems are compatible with current DoD, USAF, and Industry standards.

15.0 Software Life Cycle Management

BLACKHAWK conducts Software Life Cycle Management in conjunction with the hardware inventory process. We utilize a combination of Remedy, Tivoli®, and custom scripting to ascertain what software is loaded. Our technical managers cross reference known software licenses with those unknown, and begin a manual input of licensing from information obtained from IASOs. Once the information is entered in the database, our team works triggers to announce trouble tickets on expiring software licenses and provide advance notice to the government for budgetary and SLCM purposes.

BLACKHAWK is knowledgeable of current, supported releases of all office automation software to ensure upgrades are scheduled and carried out on time. We operate to a well-defined life cycle management process for accomplishing successful management and operations across a broad spectrum of functional areas. Team members rely on such infrastructures extensively in their management of current multi-functional projects.

BLACKHAWK's software development lifecycle processes are built upon a set of "best practices" that outline how to effectively deploy high performance software development teams. Our process provides each team member with the guidelines, templates, and tools necessary for the entire team to follow six rules: (1) Develop software iteratively, (2) Manage requirements, (3) Use component-based architectures, (4) Visually model software, (5) Verify software quality, and (6) Control software changes.

The pervasive nature of IT security threats has taught us the valuable lesson of paying continual attention to threat assessments and mitigation. Consequently, BLACKHAWK actively addresses IT security during each life cycle phase and explicitly addresses security controls during milestone reviews for each phase.

**16.0 Software Development**

BLACKHAWK currently provides software development and database maintenance for the US Army at Ft. Hood for operational applications on both unclassified and classified networks. Included in this development and maintenance are:

1. A web application with a SQL Server backend that keeps track of all officer and enlisted personnel for III Corps
2. Help Desk applications to assist in tracking trouble tickets for classified networks, as well as the Information Management Officer metrics and tracking
3. Tools used to track personnel tasking, resumes, and Internet protocol addresses tracking applications
4. Microsoft Project Server application, with customizations, and database for Ft Hood units to track all of their events and schedules
5. A web application with a database backend to track all accreditation packages for the classified networks
6. The home pages for III Corps Headquarters on the classified networks
7. Security Managers database and interface created by Blackhawk personnel keeps track of all security clearances for Ft. Hood

BLACKHAWK's core competencies in this area are database products including, SQL Server 2000, Oracle 9i, Oracle 8i, SQL and PL/SQL. We are also proficient in developing web applications using ASP.Net, JSP, Java Applets/Servlets, and VB.NET. We create most of the web applications as front ends to databases that we manage. Our development personnel are also experienced in C, C++, C#, Java, Ada, and PASCAL.

BLACKHAWK developed and maintains the functional availability simulation tool (fAST) which performs a Monte Carlo simulation of the International Space Station (ISS) functions and computes an average expected functional Availability (fA). We developed the fAST software using C++ and created a graphical user interface that takes full advantage of commercially available software (Microsoft Access). Our software engineers developed and maintain fAST using modern Configuration Management procedures and tools.

17.0 Enterprise Management Systems (EMS)

BLACKHAWK provides certified Tivoli professionals to support the Ft. Hood DOIM. We provide an experienced team in Tivoli® enterprise system management software which includes: strategic enterprise architecture planning; Tivoli® management software implementation and customization; and integration of Tivoli® management software with third party applications such as Remedy Action Request System. We covered network components that span the length and breath of Ft. Hood and four other Army and DoD installations.

Our staff also completed Tivoli® enterprise system management installations at a number of corporations including: MasterCard, Red Hat, California ISO, Stevedoring Services of America, Sutter Health, and Freightliner. These installations required Tivoli® products consisting of Framework, User Administration, Software Distribution, and Distributed Monitoring. We specialize in fast rollout and customization of the environment to meet the customer needs.

**Management Corporation**

In addition to our in-depth Tivoli® experience, our staff has installed, configured, and managed day-to-day operations for a major Tivoli® supported network at Brooks City Base, TX. We manage and implement information systems to support the Air Force Outreach Program Office (AFOPO). This network covers LAN and WAN topologies at Brooks City. We plan, design, install, and troubleshoot entire information technology network architecture and maintain computer security and integrity within AF Computer Emergency Response Team (AFCERT) guidance. Our engineers provide a diversity of support that includes: multiple desktop/laptop systems; a print/antivirus/web/system update/applications server; a network backup server, file servers; network printers; user computer hardware; software; and security training.

The Air Force Materiel Command (AFMC) is moving to a consolidated information technology environment and chose Tivoli® as their enterprise system management tool. Supporting that decision, we are the AFOPO resident experts in all aspects of Tivoli®. Our engineers use Tivoli® for inventory control, software distribution, and remote control access on all AFOPO systems, including servers.

BLACKHAWK completed the planning phase and has begun the implementation of a Tivoli® suite on a classified network that covers Ft Hood, Ft. Sill, Ft. Bliss, Ft. Carson and White Sands Missile Range. Included in this implementation are Tivoli® Management Region (TMR), Framework 5.1, TEC, Software Distribution, Configuration Management 4.1, Tivoli® Monitoring 5.1, and Tivoli® NetView 7.1.3. These are deployed on Solaris 9 operating systems running Oracle 10g. Our engineers supported one of the first Army networks to migrate from NT 4.0 to Windows 2003 Active Directory. We drew on this vast experience with Microsoft's Active Directory to push out the Tivoli® endpoints via Group Policy Objects (GPO's). By doing this we are able to prioritize unit fielding to ensure that our network infrastructure can handle software distribution.

BLACKHAWK understands that Tivoli® cannot function well without an organized framework. We have customized the infrastructure in order to efficiently manage the Tivoli® environment. With the use of Perl, shell, and Java scripting, as well as Visual Basic, Java, and C++ programming languages, BLACKHAWK can implement a customized environment based on enterprise network needs. We provide documentation of all created scripts and custom programs in both the CONOPS document and within the code itself.

BLACKHAWK engineers use these assets to ensure that all Tivoli® products are customized as needed, whether it be custom asset inventory scans to detect unauthorized software, the automation of alerts generated by Tivoli® monitoring routed through TEC (Tivoli® Enterprise Console) into Remedy Action Request System; to deploy additional endpoints; or any other custom work determined by the DOIM as necessary for the successful implementation of Tivoli® on the Ft. Hood Local Area Network.

18.0 WEB Support

BLACKHAWK provides website support to the Assistant Program Manager as-well-as technical support to the Air Force Small Business website (SAF/SB-AFOPO) which includes the Small Business Learning Center web-based training. We serve as technical adviser to the website Program Manager regarding the management and implementation of all aspects of the website. The support includes researching market practices and supporting hardware and software requirements to ensure the website remains current with industry standards, as well as DoD policies and processes. We assist in facilitating and coordinating the design, development, implementation

**Management Corporation**

and maintenance with the support contractor tasked with overall website development and maintenance.

BLACKHAWK also works as the liaison between the Air Force Program Manager and contractor personnel reviewing monthly reports for accuracy and compliance with contract task orders, and making appropriate recommendations and suggestions regarding budgetary issues. We coordinate as required with base and external agencies in maintaining and modifying the website. BLACKHAWK also assists with sustaining a distance-learning program of contracting fundamental learning modules that help all Air Force acquisition members receive centrally-based remote training in small business initiatives. These training modules contain instruction on contracting, marketing, and focused Air Force programs of assistance to small business owners, academia, small business advocacy offices, and large prime contractors nationwide.

BLACKHAWK provides technical guidance for developing and managing updates to the website. We devised and implemented a system that monitors customer feedback in support of their customer satisfaction metric. We meet with the contractor(s) and maintain documents of all tasks requested and performed. This information is made available for the review by the Program Manager, as well as the AFOPO Director and Deputy Director. BLACKHAWK actively participates in strategic planning to improve organizational and program direction and focus strategic planning tools and techniques. We provide feedback and programmatic updates to SAF/SB as appropriate in the absence of, or in support of, the website Program Manager and AFOPO Management. BLACKHAWK analyzes related issues of effectiveness, efficiency, and productivity; develops recommendations to solve problems; and applies program management principles to guide program accomplishment.

BLACKHAWK complies with security directives and policies, continually advises the Program Manager of potential problems, and recommends solutions. We keep the Program Manager apprised of all tasks requirements made to the contractor, and of the completion status of said tasks. BLACKHAWK assists the Program Manager with program reviews, task order formulation and assignment, funding projections, and conference/seminar logistical support. And, we perform special studies and projects as assigned.