2008 SBIR Phase I Technical Proposal

Data access and security in a need-to-share environment

TABLE OF CONTENTS

Black Sheep Networks

9 Prospect Hill

Tewksbury, MA 01876

Part 2 - Identification and Significance of the Problem

2.1 Identifying the Problem: Going from "need-to-know" to "need-to-share" requires new designs and a new mindset

Techniques need to be developed that address need-to-share and "browse-up" cross-domain capabilities. Current techniques for access to web resources in the military domain is based on a "need-to-know" paradigm.

As the DoD transitions from need-to-know to need-to-share, a new mindset is required. With both "need to know" and "need to share" mindsets, one must be able to answer the "who" and "what" questions. Who do we want to provide data to? The idea should be to share information and remove those pieces which need to be restricted and let the data provider determine if an individual has the criteria to access it.

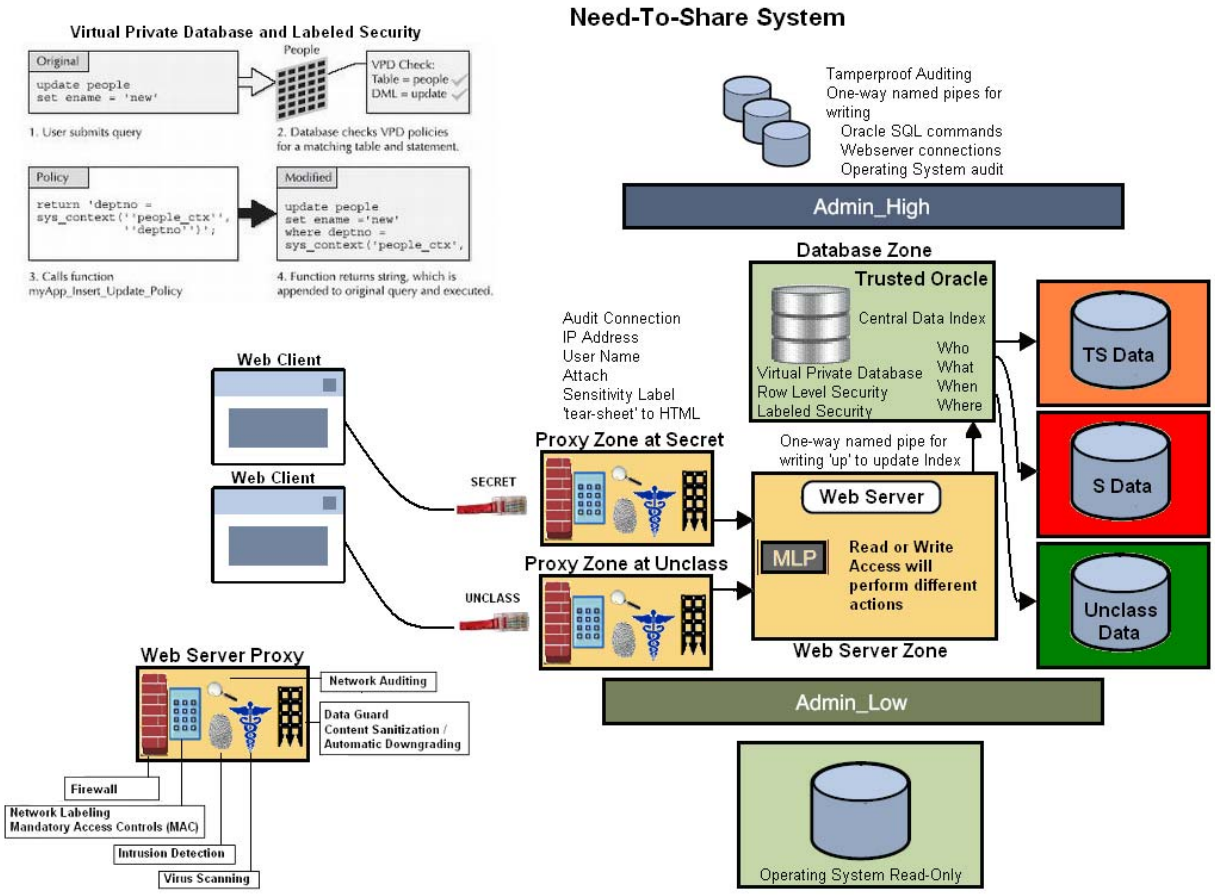
Over the short term militarily and commercially, the proposed work by Black Sheep Networks Inc. on this Technical Topic will provide an assessment of the primary complementary technologies for need-to-share cross-domain environments. By the end of the project, the data collected and analyzed in Phase I will be used to develop a working prototype of a system allowing for "browse-up" capability yet still maintaining the security, sensitivity, and integrity of the data and information being shared.

2.2 The Solution: Black Sheep Networks' "need-to-share" cross-domain system

A central data index will be how information is found, stored, and shared. The data provider will upload an object, or information, and provide which groups or users are allowed to access the data. Another user will then be able to access this shared data, however with certain safeguards based on data filtering and through the use of tear-sheets in order to downgrade information (High-to-Low). Furthermore, safeguards for sharing information from a lower classification must be controlled in order to prevent unauthorized access to higher classifications of data.

2.3 The Design

Need-to-share does not mean to break down security barriers and allow unrestricted access to data. Through the integration of existing COTS products and methodologies, a secured need-to-share environment can be obtained without bypassing all the security rules that have been put in place for decades regarding sensitive and classified material.



2.3.1 The Trusted Operating System

First, a Trusted Operating System is a requirement in order to handle different classifications of data. Solaris 10 with Trusted Extensions is Common Criteria certificated to EAL4+ with security protection profiles LSPP, RBAC, and CAPP. Solaris 10 provides network based labeling, network interface labeling, and Mandatory Access Controls.

2.3.2 The Containment and Zone Configuration

Second, a proper operating system configuration and design is needed in order to ensure the security and integrity of the system itself. Zones are used to provide containment and labeling of data. The web clients will connect to a zone that is running a web-based proxy server. This proxy server will add an HTML tear-sheet providing user and sensitivity label information. The proxy server will then forward the HTML request to an internal WebServer zone. The WebServer zone will communicate with the Database Zone in a read-only mode via TCP sockets or write-mode via a single direction pipe that will allow data to go 'up' but not the other direction. Writing up is possible using named pipes which are loopback mounted into higher-level zones on Solaris 10. This unidirectional conduit allows for implementing a one-way guard and for tamper-proof logging.

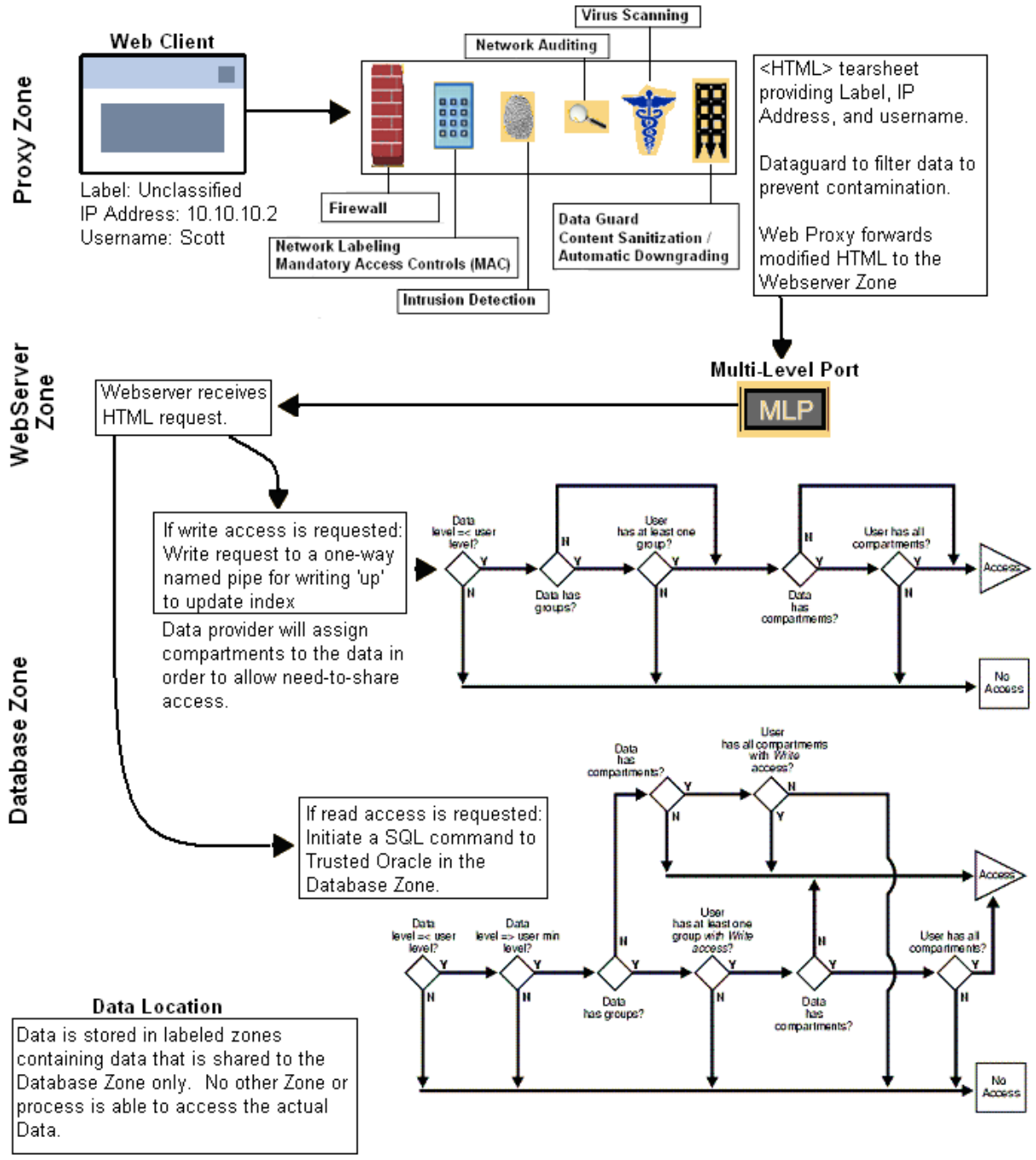
2.3.3 Low-to-High writing 'up'

One-way named pipes (FIFOs) located in the WebServer Zone are associated with a file system entry that allows unrelated processes, located in the Database Zone, to find and open a named pipe for communication. Discretionary and mandatory access controls are enforced when the named pipe is opened and FIFO special file created based on the named pipe's permission bits and sensitivity label.

The sensitivity label of the process writing the data is associated with each byte of data sent down the pipe. The mandatory access policy for writing to and reading from a named pipe is read-equal and write-equal.

2.3.4 The Database

The final part of the environment is the database storing the central index itself. Trusted Oracle, working with Trusted Solaris, provides the ultimate in labeled security (MLS) by providing Virtual Private Databases and Labeled Rows. The database is given "who" and the database provides "what" shared information the user is allowed to access. The database will have absolutely no access to any network and can only communicate to the WebServer zone via special TCP ports and one-way named pipes (FIFOs). All Database TCP communications will be read-only. Any database writes, creations, or updates are written to a file and a special process on the Database zone will gather this information, sanitize, and import it into the database. Deletions are not possible, only updates to make the object or information not to be shared.


Proxy Zone
Web Client
Label: Unclassified
IP Address: 10.10.10.2
Username: Scott
Virus Scanning
Network Auditing
Firewall
Network Labeling
Mandatory Access Controls (MAC)
Intrusion Detection
Data Guard
Content Sanitization /
Automatic Downgrading
<HTML> tearsheet providing Label, IP Address, and username.
Dataguard to filter data to prevent contamination.
Web Proxy forwards modified HTML to the Webserver Zone
Multi-Level Port
MLP
WebServer Zone
Webserver receives HTML request.
If write access is requested: Write request to a one-way named pipe for writing 'up' to update index
Data provider will assign compartments to the data in order to allow need-to-share access.
Data level =< user level?
Data has groups?
User has at least one group?
Data has compartments?
User has all compartments?
Access
No Access
Database Zone
If read access is requested: Initiate a SQL command to Trusted Oracle in the Database Zone.
Data has compartments?
User has all compartments with Write access?
Access
Data level =< user level?
Data level => user min level?
Data has groups?
User has at least one group with Write access?
Data has compartments?
User has all compartments?
No Access
Data Location
Data is stored in labeled zones containing data that is shared to the Database Zone only. No other Zone or process is able to access the actual Data.

2.3.5 Virtual Private Database and Row Level Security

Trusted Oracle's Virtual Private Database's row-level security (RLS) allows the restriction of access to records based on a security policy implemented in PL/SQL. A security policy simply describes the rules governing access to the data rows. This process is done by creating a PL/SQL function that returns a string. The function is then registered against the tables, views, or synonyms you want to protect by using the DBMS_RLS PL/SQL package. When a query is issued against the protected object, Oracle effectively appends the string returned from the function to the original SQL statement, thereby filtering the data records. This security is implemented so that it is transparent and can not be subverted.

2.3.6 Labeled Storage and HTML Dataguard/Filtering

The database will write data to labeled storage locations on the system based on the data provider's sensitivity label. Markings of this sensitivity label will be stored in the Trusted Oracle database index and will be part of the HTML communication via a 'tear-sheet' metadata containing classification and other information. The HTML page will then be sent back to the requesting user complete with this metadata, which will be used for filtering through the dataguard located in the WebServer Proxy Zone.

Part 3 - Phase 1 Technical Objectives

Objective 1: Research and understand the proposed environment for a browse-up cross-domain solution

Contact the program manager and discuss the problem in full detail. How is the current sharing of information implementation being performed? Will a central database index be a viable option for the DoD? Perform research on past and present cross-domain systems and their failures for "browse-up" capabilities. Discover how these capabilities have failed and how to overcome these problems in a secured approach with sensitive data in a shared environment.

Objective 2: Research and define hardware and the Operating System used

Discover possible alternative Operating Systems that will facilitate the "need-to-share" paradigm. Certain COTS operating systems may not be Common Criteria certified for use in the DoD. How will a particular Operating System provide the foundation of a "need-to-share" system?

Objective 3: Research and define a Central Data Index database design and configuration

Which Database software is best to use in a "need-to-share" environment? Are trusted features needed for ensuring there is no contamination of classifications of data? How will features of the database allow information sharing and keeping classified data integrity intact?

Objective 4: Research and define how the Operating System and Central Data Index will interact in order to provide sensitivity labels and data filtering of content

How will the Central Data Index and Trusted Operating System interact and be integrated? What hooks or customized code will be required to integrate? What modifications will need to be performed in order to meet various DoD security requirements, SRR/STIG scripts and NSA OS hardening guidelines, etc..?

Objective 5: Research and define what types of metadata is needed and how they will be utilized in the design

What information is needed in relation to each piece of data? Which information will be automatically assigned (Mandatory) or where the data provider will input? How will this metadata be located in the Central Database Index and how will it affect the capability to provide need-to-share?

Accomplishment of all the technical objectives will allow Black Sheep Networks to proceed to Phase II, which includes the development of a working prototype of a "browse-up" cross-domain system.

Part 4 - Phase 1 Work Plan

The following tasks will occur in serial immediately upon SBIR award:

Task	Staff	Start	Finish	Task Details	Milestone
Identify Environment	Kevin Caldwell Romande Carter	Week 1	Week 4	Research Providing an Overview Design	Initial High-Level Design is completed
Hardware and OS Design	Kevin Caldwell Romande Carter	Week 5	Week 10	Full Detail and Design of Hardware and Operating System including Information Security for DoD requirements	Multi-Level (MLS) Operating System Design is completed and able to pass DoD Security Requirements
Database Design	Kevin Caldwell	Week 11	Week 20	Full Detail of Database and its configuration with rows and Labeled Security	MLS Security Database Design for "need-to-share" is completed
OS and Database Interaction Design	Kevin Caldwell Romande Carter	Week 21	Week 28	Merging the Multi-Level Operating System with the Multi-Level Security Database and how they will interact. Custom Software designed for Dataguarding and Filtering functions.	Integration of OS and Database Designs complete with Dataguard and custom software features that will be needed
Metadata and Information Utilized	Kevin Caldwell	Week 29	Week 34	Actual "need-to-share" design based on a MLS/MILS base framework (The OS and Database) that provides the ability to allow "browse-up" capabilities. Putting it all together.	Complete "need-to-share" system Designs are complete

Deliverables

a. Kickoff meeting within 30 days of contract start

b. Progress reports

c. Technical review within 6 months

d. Final report with SF 298

Part 5 - Related Work **(We have done this before)**

Black Sheep Networks has worked with SPAWAR, NAVSEA, and the IRS through larger defense companies such as Eagen McAllister and Raytheon. The successes of these agencies specific cross-domain solutions were only possible with Black Sheep Network's innovative technical abilities in Information Security and Cross-Domain solutions utilizing Trusted Solaris. Most recent work was designing a Trusted Solaris system to meet requirements and cross-domain abilities for the JFIRES (Joint Force Interoperability and Requirements Evaluation SupraCenter) program that provides a multi-mission Joint Battlespace environment. Past work includes preparing a Trusted Solaris system for DCID 6/3 PL4 accreditation (and completing the FISMA accreditation process by ONI and DIA accreditors) as a cross-domain (high-low) dataguard for submarine Weapon Combat Systems. Current work involves a new iteration of the Navy's submarine combat control systems (NUWC/NAVSEA) with Solaris 10 and Trusted Extensions for DODIIS and DCID 6/3 accreditation as a cross-domain solution.

Part 6 - Relation with Future R&D

The methodology developed by Black Sheep Networks for the "browse-up" cross-domain solution will be easily adaptable to any future modalities. The proposed methodology developed under Phase I can be modified to work in any type of information sharing environment.

Part 7 - Commercialization Strategy

Black Sheep Networks seeks to develop a Cross-Domain system design that can be marketed to any industry requiring sharing of information and ensuring data integrity and security. For example, industries such as healthcare can benefit by allowing a patient to view his/her full medical information yet only share parts of this information to Insurance Companies. Another industry that can benefit from a need-to-share cross-domain solution would be Law Enforcement by sharing information to an attorney, or member of the press, specific information about a case yet not reveal the entire case.

Part 8 - Key personnel

Kevin Caldwell - Technical Investigator, Chief Consultant

Kevin Caldwell brings a vision of providing high quality Information Security services for both corporations and the Government. He has over 12 years of start-up and corporate experience. Mr. Caldwell has held several roles with his career in Information Technology. His roles have ranged from a UNIX administrator, Manager, Director, and even a co-founder of a web-hosting company and an Information Security Consultancy. He has worked with several companies large and small from RSA Security, Nortel Networks, RiverDelta Networks, Motorola, Paper Exchange, Arris, Bandwidth Center, Armored Servers (http://www.armoredservers.com), and Black Sheep Networks (http://www.blacksheepnetworks.com). Government agencies include SPAWAR Space and Naval Warfare, NUWC, NAVSEA, and the Internal Revenue Service. Mr. Caldwell has also worked for over 6 years securing, armoring, and providing cross-domain Government and Military solutions. Mr. Caldwell brings expertise in UNIX security, network security, and Government Security as well as the business mindset needed in today's security designs.

Technical Investigator Relevant and Recent Experience:

Nov 2001 – Present **BLACK SHEEP NETWORKS INC.**
Chief UNIX Security Consultant
Tewksbury, Massachusetts
http://www.blacksheepnetworks.com

- Founder of data/information security consulting corporation
- SECURITY Consulting includes:
  - Penetration Testing
  - Firewall and DMZ configuration
  - Vulnerability Analysis
  - Operating System Hardening
  - Cyber Forensics
  - System and Network Security Design
  - Disaster Recovery Planning
  - FISMA / Government DCID6/3 Protection Level accreditations
- UNIX Consulting includes:
  - Upgrades and new Installations with:
    - Solaris, SGI IRIX, AIX, variations of Linux, and HPUX, TSOL
  - Application installations such as:
    - Rational ClearCase, Veritas VM (VXFS), Oracle,
    - Apache, LDAP, NIS, DNS, Checkpoint FW-1
    - CA eTrust Access Control, RSA ACE/Server (SecurID)

•Some recent clients that Kevin has performed services for: (LONG and SHORT term)

RAYTHEON [Portsmouth, RI] 2/2004 – Present

•Secret Clearance at Raytheon in Portsmouth, RI

[Tech Insertion TI08] 9/2007 – Present

•Designed next generation NTDS submarine interface gateguard with Solaris 10 and Trusted Extensions utilizing Containers, aka Zones, labeling and Mandatory Access Controls (MAC) to meet DCID6/3 PL4 accreditation.

•RedHat Linux RHAS 5 minimization and armoring

[Tech Insertion TI06] 9/2006 – 8/2007

•Designed system based on NTDS submarine interfaces with Trusted Solaris 8 to meet DCID6/3 PL4 and JDISCIS by ONI/SSO NAVY (Office of Naval Intelligence) and DITSCAP accreditation (STIG)

•Designed PKI authentication using keys instead of passwords for entire Weapon Control submarine network

•RedHat Linux RHAS 4 minimization down to 100mb filesystem

•Computer Associate's eTrust UNIX Access Control implementation

•SUN SunScreen firewall on Trusted Solaris 8

•Implemented iSCSI SAN environment, along with GFS filesystem and RedHat Cluster Servers

•Designed unique Trusted Solaris 8 system to be defined as Controlled Interface, aka appliance, with no interaction or logins possible.

•Designed centralized shipboard virus scan gui in TCL/tk

•Designed development lab maintenance, cleanup, and usage admin GUI in TCL/Tk

•Assisted integrating TSOL functionality involving label downgrades into existing Weapons Control code at Raytheon

[Tech Insertion TI04] 2/2004 – 8/2006

• Designed a Centralized Password Accountability and Distribution software application developed in TCL/Tk for cross-platform independence. Implemented on Submarine Combat Systems, providing logging and auditing of user, group, and password schemes using encrypted network tunnels and an embedded SQL Database Engine.

•Provided Information Assurance for Submarine Combat Systems

•Hardening of HPUX 10.20 and 11.0, Trusted Solaris 8, RedHat Linux 7.3 and 9.0, and Windows 2000. Design and creation of OS Armoring scripts.

•W2K Armoring application designed with TCL/Tk

to provide a GUI interface. Use of Freewrap to compile TCL/Tk code into an self-contained executable format.

- Usage of DoD STIG Security Guidelines and scripts
- Setup of Symantec Enterprise Security Manager (ESM)
- Setup and support of Symantec Intruder Alert (ITA)
- Design of Central Virus Scan for Linux/HPUX platforms
- Full Customization of Symantec ESM for security settings
- Deployed and Administered Trusted Solaris 8 environment
- Provided Trusted Solaris 8 (x86) Support

RAYTHEON ***Woburn, MA Location*** 10/2006 – 12/2006

- Jfires (Joint Fires) platform, Designed and implemented Trusted Solaris 8 on several SUN Fire v440 systems to meet special environment restrictions and requirements for NISPOM PL3 accredidtation by DIA.
- Full documentation for Design and meeting PL3 accreditation

Sunbelt Network Inc. 8/2004 – 11/2007

- Provided Oracle 10g installation, configuration and support on SUN E4500, and SUN Fire v880 servers.
- EMC Symetrics Storage devices configure and maintain

EMB Statistical Solutions, LLC 1/2004 – 3/2004

- Contract research organization providing data Management and statistical analysis of Clinical research data
- Design and Setup of data storage system
- SUN Hardware and Solaris 10 OS Design

SPAWAR (Space and Naval Warfare) [Charleston, SC] 3/2003 – 2/04

- Secret Clearance at SPAWAR Systems Center [DoD]
- Lead INFOSEC UNIX engineer with Tiger Team Working with SPAWAR Information Warfare agency [DoD]
- Intrusion Detection and Policy Enforcement
- SPAWAR and IRS (Internal Revenue Service) Security assessments
- Designed Software Development Process for IRS UNIX LEM
- Setup/Maintained Configuration Management with ClearCase
- Migrate development code to ClearCase
- Established ClearCase vobs for four development projects
- Established backup procedures
- Established procedures for check-in/out, setview, etc.

- Established build and integration procedures
- Provided training as needed
- Setup development environment consisting of AIX, HPUX, BSDi, Solaris, Linux, and Tru64 operating systems
- Created Software Development portal for UNIX LEM Checker
- Managed development of UNIX System Security Scanner for IRS
- Design and Implement NTP securely with Access control and Authentication
- NTP and Sendmail Security Documentation
- ISS (Internet Security Scanner) Scans
- eTrust Access Control and Audit Deployment
- CVS and Configuration Management Deployment
- Setup Coding, BugTracking, and Testing Environment
- Documentation Writing and Management
  - Standard Operating Procedures
  - Technical Documentation

Romande Carter – UNIX Technical Engineer

Romande Carter has more than nine years of experience with UNIX systems administration, optimization, and performance analysis. He has worked with companies large and small such as Nortel/Arris, Fleet Bank, and Evergreen Investments. His UNIX Administration background with Financial companies has proven to be a tremendous value in regards with UNIX Information Security.

Part 9 - Facilities/Equipment

All proposed work will be completed at the Black Sheep Networks' office in Tewksbury, MA. Black Sheep Networks maintains a computer security research datacenter and has the facilities and equipment to research and develop Information Security solutions and technologies.

Part 10 - Subcontractor and Consultant Involvement

Black Sheep Networks will not need any subcontractor or consultant involvement on this project for Phase I.

Part 11 - Prior, Current or Pending Support of Similar Proposal or Award

Black Sheep Networks has no prior, current, or pending support for a similar proposal.