

# **Trusted Facility Manual (TFM) for Broadsword**

**Version 3.1**

**September 2002**

**Prepared for:**

AFC2ISRC/A26

Langley Air Force Base, VA 23665

**Prepared by:**

Air Force Research Laboratory, Rome Research Site

AFRL/IFEB

32 Brooks Road

Rome, NY 13441-4114

## **VERSION NOTE**

This document is the current version of the Broadsword 3.1 Trusted Facility Manual, superceding the Broadsword 3.1 Trusted Facility Manual dated 17 June, 2002. This document was updated to reflect the changes in functionality added with the 3.1.x patch to the 3.1 software.

# TABLE OF CONTENTS

<b>VERSION NOTE .....</b>	<b>II</b>
<b>TABLE OF CONTENTS.....</b>	<b>III</b>
<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 INTRODUCTION TO THE BROADSWORD TRUSTED FACILITY MANUAL (TFM) .....	1
1.1.1 Purpose of the manual.....	1
1.1.2 Recommended use of the manual.....	1
1.2 AUDIENCE .....	1
1.3 SCOPE.....	1
1.3.1 System Description .....	1
1.3.2 Gatekeeper.....	2
1.3.3 Keymaster .....	6
1.3.4 Trusted Transfer Agent (TTA) .....	8
1.3.5 The Broadsword Client.....	9
1.4 PRODUCT TRADEMARK REGISTRATION.....	14
1.5 REFERENCES .....	26
<b>2 SYSTEM SECURITY OVERVIEW.....</b>	<b>27</b>
2.1 SYSTEM ENVIRONMENT .....	27
2.2 SYSTEM AND SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES.....	27
2.3 SYSTEM USER ACCESS POLICY .....	33
2.3.1 User Access Controls.....	33
2.3.2 Assignment and Control of Authenticators .....	33
2.3.3 IS User Access .....	34
2.3.4 Privileged User Access.....	34
2.3.5 Password Changes .....	34
2.3.6 Password Generation .....	35
2.3.7 Number of Allowed Login Attempts.....	35
2.3.8 Account Logout.....	35
2.4 USER GROUPS AND ACCESS RIGHTS .....	35
2.4.1 User Groups .....	36
2.4.2 System Files.....	37
2.4.3 System Access Rights .....	37
2.4.4 Audit Log Access .....	37
2.4.5 Privileged Users .....	38
2.4.6 DAC/MAC.....	38
<b>3 SECURITY RELATED FEATURES AND PROCEDURES.....</b>	<b>39</b>
3.1 PROTECTION OF THE SECURITY SUPPORT STRUCTURE.....	39
3.2 SECURITY FEATURES AND ASSURANCES.....	39
3.2.1 Incident Reporting .....	39
3.2.2 Remote Access .....	39
3.2.3 Change Control.....	40
3.2.4 Configuration Management.....	40
3.2.5 Security Features.....	40
3.2.6 System Startup .....	40
3.2.7 System Shutdown .....	40
3.3 AUDITING.....	41
3.3.1 User-level Auditing.....	41
3.3.2 Audited Information.....	58
3.3.3 Audited Activities.....	58

FINAL

- 3.3.4 *Audit Review* ..... 58
- 3.3.5 *Audit Handling* ..... 59
- 3.4 MARKING AND LABELING ..... 59
  - 3.4.1 *Hardware*..... 59
  - 3.4.2 *Storage Media*..... 59
  - 3.4.3 *Hardcopy Output* ..... 59
- 3.5 SANITIZATION AND DESTRUCTION ..... 59
  - 3.5.1 *Hardware*..... 59
  - 3.5.2 *Software*..... 59
- 3.6 SOFTWARE SECURITY PROCEDURES ..... 59
  - 3.6.1 *Procurement* ..... 60
  - 3.6.2 *Impact Evaluation*..... 60
  - 3.6.3 *Virus and Malicious Code Protection* ..... 60
  - 3.6.4 *Maintenance* ..... 60
- 3.7 MEDIA MOVEMENT ..... 60
  - 3.7.1 *Into and Out of Secure Facility*..... 60
  - 3.7.2 *Copy/Review/Release*..... 60
- 3.8 HARDWARE CONTROL ..... 60
  - 3.8.1 *System Transport* ..... 60
  - 3.8.2 *System Relocation*..... 61
  - 3.8.3 *Control/Operation/Maintenance* ..... 61
  - 3.8.4 *Hardware Acquisition*..... 61
- 3.9 WEB PROTOCOL AND DISTRIBUTED/COLLABORATIVE COMPUTING ..... 61
  - 3.9.1 *Web Server Security*..... 61
  - 3.9.2 *Mobile Code* ..... 61
  - 3.9.3 *Executable Code* ..... 61
  - 3.9.4 *Collaborative Computing* ..... 62
  - 3.9.5 *Distributed Processing* ..... 62
- 4 BACKUP POLICY AND PROCEDURES..... 63**
  - 4.1 STORING ARCHIVED AUDIT LOG RECORDS USING OFFLINE TAPE STORAGE..... 63
    - 4.1.1 *Storing Audit Logs*..... 63
- 5 RESTORATION POLICY AND PROCEDURES ..... 65**
  - 5.1 RETRIEVING ARCHIVED AUDIT LOG RECORDS USING OFFLINE TAPE STORAGE ..... 65
    - 5.1.1 *Retrieving Broadsword audit logs* ..... 65
- 6 KNOWN VULNERABILITIES AND RISK MITIGATION APPROACH..... 67**

# 1 INTRODUCTION

## 1.1 Introduction to the Broadsword Trusted Facility Manual (TFM)

### 1.1.1 Purpose of the manual

This manual is intended to:

- Guide the secure configuration and installation of the system
- Guide the operation of the system in a secure manner
- Enable administrative personnel to make effective use of the system's privileges and protection mechanisms.
- Issue warnings about possible misuse of administrative authority

### 1.1.2 Recommended use of the manual

This manual should be used to:

- Review skills and system background necessary for security and system administrator personnel.
- Suggest additional manuals, reference material, and standards needed by security and system administrator personnel

## 1.2 Audience

This document is intended only for privileged users such as system/network administrators, ISSMs, Information System Security Officers (ISSOs), etc.

## 1.3 Scope

*Specify the limitations of security scope and guidelines for the security administrator to operate the system in a secure and effective manner. Also provide information about the environment, roles, and responsibilities that guide security administrator use of the security features and detailed system security features and procedures information for privileged users.*

### 1.3.1 System Description

Broadsword implements a multi-tier architecture supporting a single, seamless interface that is secure and administratively manageable. The Broadsword architecture contains four functional components. These components collectively act on behalf of all parties (ISSO, System Administrator, and User) and are tailored to meet the connectivity requirements of the site. **Table 1.1** provides an overview of each component:

Functional Component	Purpose
Gatekeeper	Provides single interface to various sources for query, retrieval, and product request/delivery. It also provides a single point in which users are authenticated and all actions audited. (Section 1.3.2)
Keymaster	Maintains and distributes a global map of published data sources to permit remote Gatekeepers' users access, assuming both the data source's local Gatekeeper and the remote Gatekeepers are registered with the same Keymaster. In the existing environment, there is only one Keymaster for each Security Domain. (Section 1.3.3)
Trusted Transfer Agent (TTA)	TTA allows the user to query a lower security domain and retrieve products without human intervention while crossing between security domains. It is a separate package of code that also relies on the installation of an ISSEGUARD server. . This is an optional addition to the standard Broadsword install. (Section 1.3.4)
Broadsword Client	Graphical user interface which implements the Client/Gatekeeper API and provides ISSO, System Administrator and General Searching/Product Producer capabilities (Section 1.3.5)

**Table 1.1 – Summary of Broadsword Functional Components**

### 1.3.2 Gatekeeper

The Gatekeeper component is the heart of the overall architecture. It is a robust, thin layer of software which performs a variety of internal functions, including processing users' queries, auditing, communicating with various sources, interconnection with other Gatekeepers, maintaining system status, and collection/compilation of results. The Gatekeeper supports a single Application Programmers Interface (API) for developers to access the functionality provided and to create applications. The API is based on a simple message passing mechanism and is divided into three sections: (1) User, (2) Administration, and (3) ISSO. A fourth section is the various plugins that connect Broadsword with the datasources. **Figure 1.1** shows the overall architecture of the Gatekeeper.

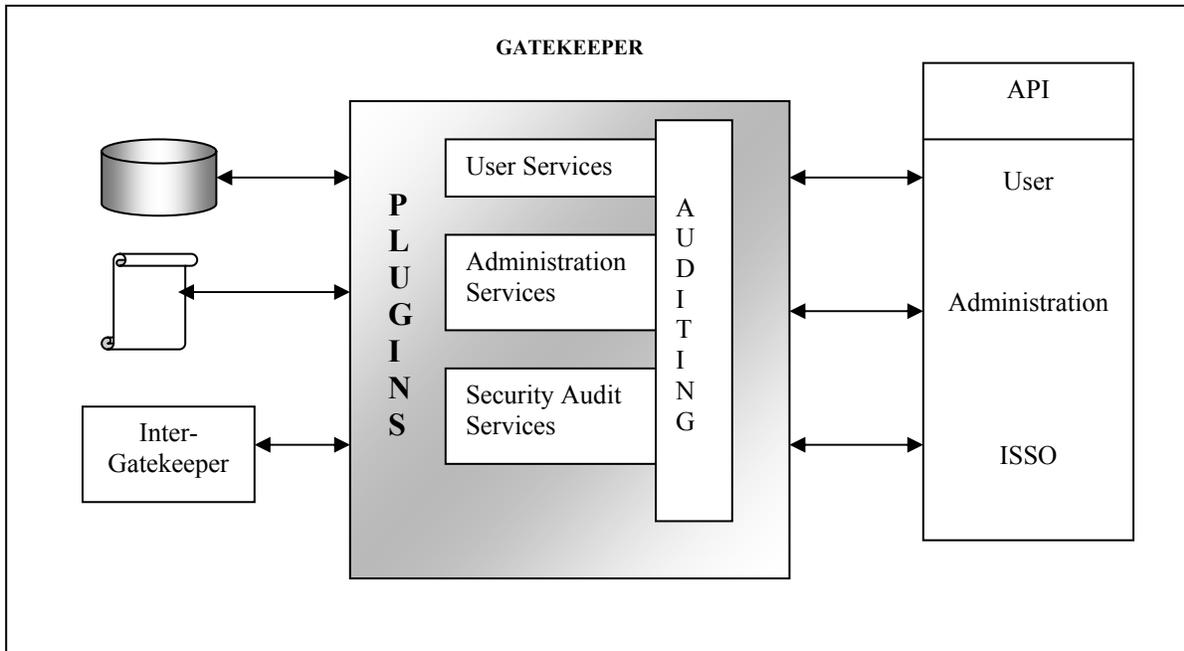


Figure 1.1 – Overall Gatekeeper Architecture

### 1.3.2.1 User Services

The Gatekeeper provides support for the processing of user request, collating the results, delivering products, and converting/compressing supported imagery. User request can be spatial or SQL based. The availability of request options is dependent upon the sources connected and what each source supports. Once a request has been submitted, the Gatekeeper audits the request, forwards it to all appropriate sources via plugins, and waits for each of the sources to respond. When the Gatekeeper receives responses from each source, it combines any and all results into a single response, builds an audit record, and forwards the response to the requester. **Figure 1.2** summarizes the major functionality provided by the Gatekeeper through the User Services portion of the interface.

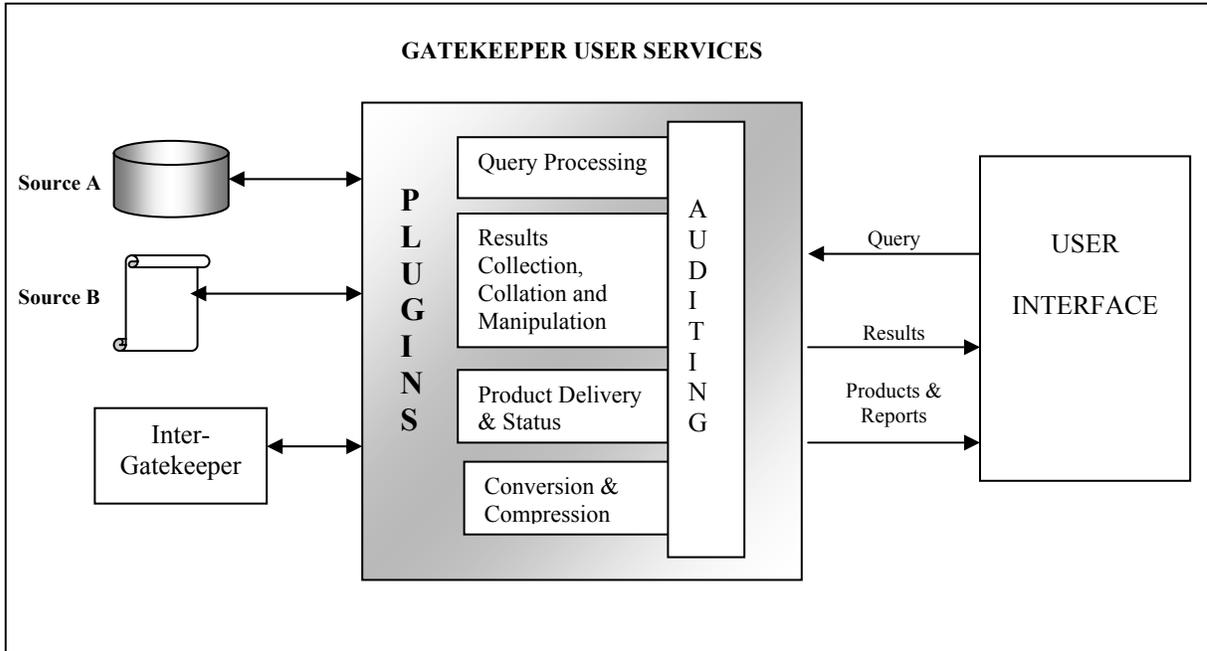


Figure 1.2 – User Services

Some of the sources that are connected to the Gatekeeper may support the ordering and delivery of products. Products include reports from database sources, messages, documents, video clips, maps, and images. Delivery mechanisms from the individual sources include non-real-time mail order delivery, FTP delivery, or near-real-time FTP delivery.

A number of the imagery sources provide varying degrees of conversion and compression support. As a minimum, each source stores imagery using the National Imagery Transfer Format (NITF) 2.0. This standard supports many levels of compression, bit sizes, and storage formats. There are a number of commercial products that can view the full range of NITF storage options. To provide for a wider range of users (those who do not have nor wish to pay for a special application), the Gatekeeper provides conversion support to TIFF 6.0 and JPEG formats. Additionally, when users request NITF 2.0 products from an IPL datasource, the Gatekeeper will repack the NITF header. This will update the NITF product's header information with the appropriate metadata currently stored in the IPL datasource.

### 1.3.2.2 Administration Services

Under Administration Services, the Gatekeeper provides an interface for user maintenance, system statistics, and system configuration. Access to the functionality provided by these services is limited to authorized users only. Under User/Group Maintenance, the system administrator creates and configures user accounts and groups. The mode is a combination of CSE-SS/AFDI and the Broadsword Administrative Interface. User account creation and password maintenance is managed through CSE-SS

FINAL

or AFDI, while Broadword roles and source permissions are maintained through the Broadword Administration Interface. Each user can be assigned to one or more groups and have access to various sources. Members of groups share sources and roles assigned to the group. Groups are created and configured through Group Maintenance.

System Statistics provides Gatekeeper statistics, including a listing of the most frequently accessed products and the most frequently processed queries. In System Configuration, the system administrator configures the Gatekeeper, adds/edits/removes backside sources, defines values for attributes and establishes connectivity with other Gatekeepers through registration with the Keymaster. **Figure 1.3** summarizes the major functionality provided by Administration Services.

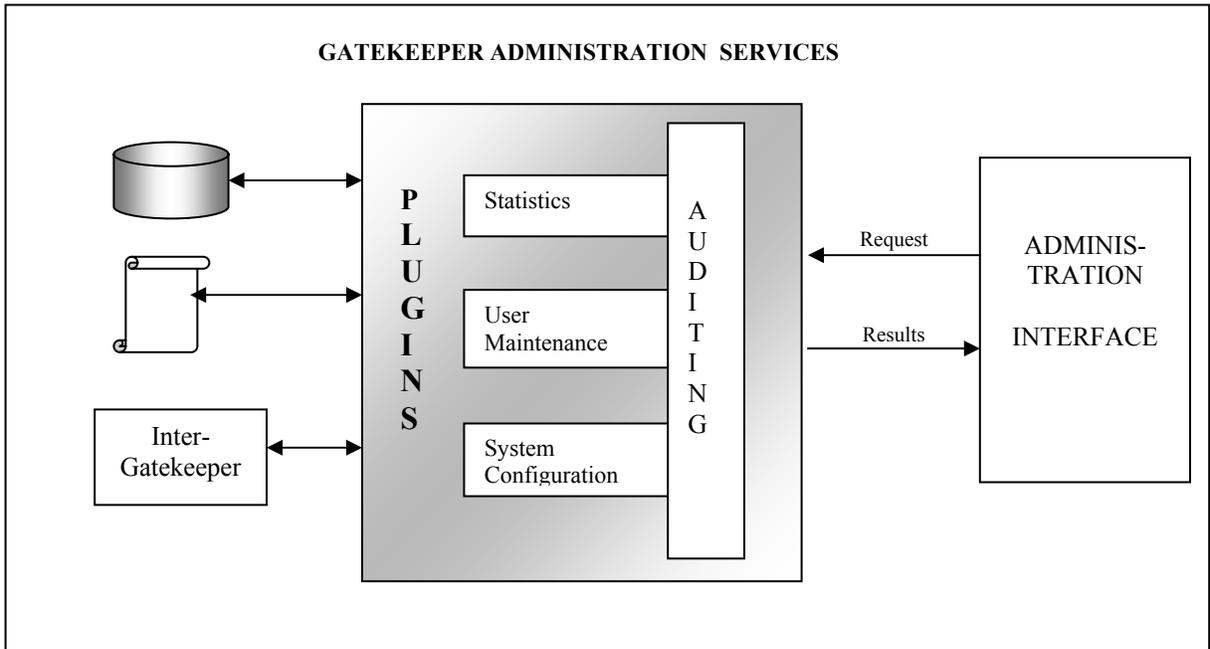


Figure 1.3 – Administration Services

### 1.3.2.3 Security Audit Review

The Security Audit Review interface provides the ability to view, archive, and remove audit information. Those records that have been archive are also available for review. All audits are stored in a database. Broadword version 3.1 offers Sybase as the database engine during the installation. Security records may be filtered based on any one event, username, and/or time range. **Table 1.2** provides a listing of the events that are audited by the Gatekeeper.

<b>Gatekeeper Security Audits</b>		
<b>User Events:</b>		
Catalog Request	Transfer Request	User Logged Out
Query	User Logged In	
<b>Administration Events:</b>		
Gatekeeper Stopped	Removed Group	Added Discretionary Access Control (DAC)
Get Column Attributes	Removed Group Member	Added Group
Initiate Stream Request	Remove Source	Added Group Member
Modified Element	Set Source Parameter	Added New Source
New or Updated Gatekeeper Info	Set User DAC	Added User Privileges
Register our Gatekeeper With Keymaster	Terminate Stream Request	Clear Statistics
Removed DAC	Update Daemon Status	Gatekeeper Started
Removed Remote Gatekeeper	Modified Group	Removed User Privileges
Client Profile Management	Client Profile Queue Maintenance	
<b>ISSO Events:</b>		
Audit Dump	Got Audit Report	Delete Audit

Table 1.2 – Summary of Security Audits

The certifying authority uses the audit trail dumps, in conjunction with the system audit logs, to validate security auditing requirements. Broadsword relies on three Sybase audit log formats (Audit Report, Product Request Report, and Query Report) to generate audit reports. See TFM Attachment II – ISSO User’s Guide for more information on Broadsword Audit Logs.

#### 1.3.2.4 Plugins

Plugins are the segments of code which reside between the Gatekeeper and a specific datasource. Examples include the IPL25 Plugin, which interfaces with IPL 2.5 and 2.5.1, or MIDB Plugin, which interface with the MIDB. The Gatekeeper installs with a full set of plugins for all datasources that it currently supports. These plugins are not run until the Broadsword Administrator configures a backside source of the appropriate type through the Administrative services. One copy of each configured plugin is run, regardless of how many instances of that type of datasource is configured. Each of the above figures (Figure 1.2 or 1.3) demonstrates the logical placement of the plugins.

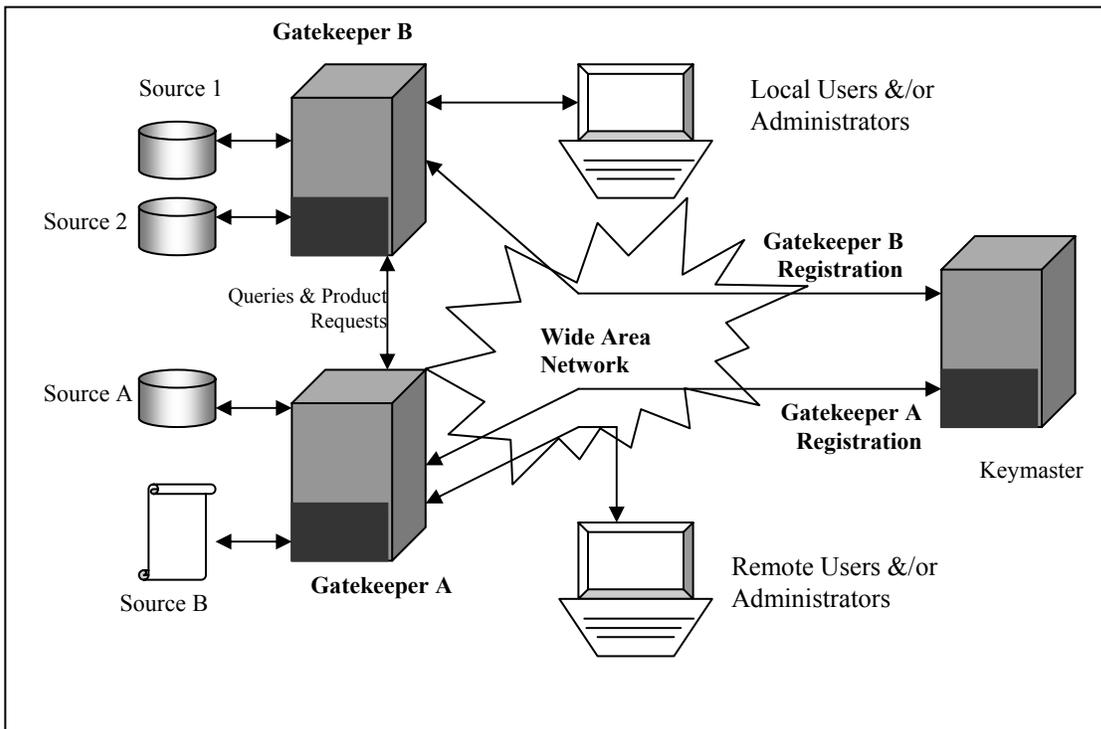
#### 1.3.3 Keymaster

Sources at a site can be made available to other sites through the Gatekeeper to Gatekeeper connection. Gatekeepers have the ability to communicate with each other and

FINAL

their respective sources as long as each site has registered their Gatekeeper with a Keymaster. The Keymaster manages a list of all Gatekeepers and their sources that have registered with it. During the registration process, a Gatekeeper receives the global map. The global map identifies all other Gatekeepers and sources. Queries and product requests performed between the available Gatekeepers do not involve the Keymaster. Changes in a specific Gatekeeper's configuration are propagated up to the registered Keymaster and are then propagated back down to all other Gatekeepers. **Figure 1.4** shows the Broadsword architecture with two Gatekeepers and a Keymaster.

Note: Keymaster POC information for the required security domain can be obtained by contacting the Centralized Help Desk (CHD) for Intelligence Data Handling Systems (IDHS) at DSN: 587-4347 or Commercial (315) 330-4347. The information can be obtained from the Broadsword Installation Guide. The install worksheet is located in Table 2.1 #68.



**Figure 1.4 – Gatekeeper/Keymaster Architecture**

The Keymaster uses a subset of the API libraries provided as a part of the Gatekeeper. Specifically, it uses the login process, its associated user administration capability and ISSO functionality. **Table 1.3** provides a list of auditable events within the Keymaster.

UNCLASSIFIED

<b>Keymaster Security Audits</b>		
<b>User Events:</b>		
User Logged In	User Logged Out	
<b>Administration Events:</b>		
Accept Registration from Remote Gatekeeper	Keymaster Stopped	Remove Remote Gatekeeper
Added Discretionary Access Control (DAC)	New or Updated Gatekeeper Info	Remove User Privileges
Set User DAC	Removed DAC	Added User Privileges
Update Daemon Status	Keymaster Started	
<b>ISSO Events:</b>		
Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 1.3 – Summary of Security Audits

### 1.3.4 Trusted Transfer Agent (TTA)

The Gatekeeper and Keymaster provide a powerful infrastructure for the interconnection of information sources within a single Community of Interest (COI) and a single security domain. TTA brings together this powerful infrastructure and the multiple security level (MSL) capability provided under the Information Support Server Environment (ISSE) Guard. TTA provides any authorized user within the Gatekeeper COI operating at the high-side security level the ability to access, query, and pull information from a low-side COI.

#### 1.3.4.1 Overall Architecture of TTA

The TTA High Gatekeeper and TTA Low Gatekeeper configurations include a number of processes that must work continuously and cooperatively in order to ensure proper operation of the TTA system. If a serious error is detected in any TTA process on either the high side or the low side platform, action is taken automatically to shutdown either the high side or low side TTA processes, quickly, completely, and correctly. This ensures that no information will inadvertently pass through the TTA because processes are not working correctly, and protects against the Unix file system directories, used in various locations within the TTA system, from becoming overloaded. Once TTA is started, high side and low side process controller components of TTA continuously monitor the status of all TTA high side and low side processes respectively. If one of those processes exits for any reason the process control recognizes that fact and signals all other TTA processes to gracefully exit thus bringing down the high side or low side of the TTA completely. When this event occurs, messages are written to the system log allowing the TTA Administrator to determine when and why the event occurred. **Figure 1.4** displays the overall Gatekeeper/TTA architecture.

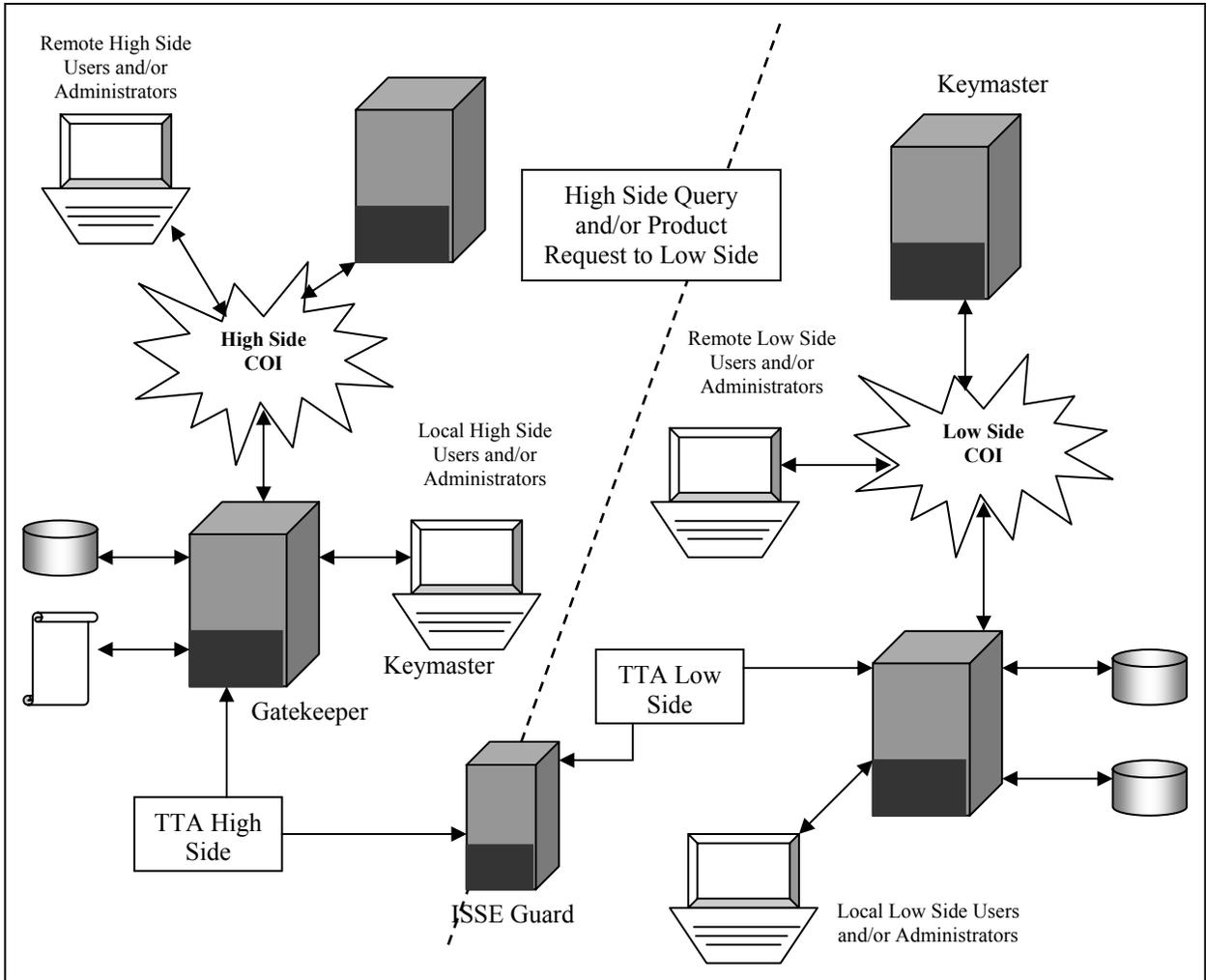


Figure 1.5– TTA Architecture

### 1.3.5 The Broadword Client

Broadword provides a User Interface to access the Gatekeeper and local data sources. It is Web-based and supports multiple roles. Roles are assigned on an individual user or group basis. These roles automatically include the General User Role (aka ‘Searching’ role), and may include one or more of the following: Producer, Managed Producer, Catalog Manager, Administrator, and/or ISSO.

The user will log into the system from the main screen. Based on the user’s login, the main screen will be tailored to the roles that have been assigned by the site System Administrator. The following paragraphs provide an overview of the functionality supported through the client interface. **Figure 1.6** shows the overall User Interface Architecture.

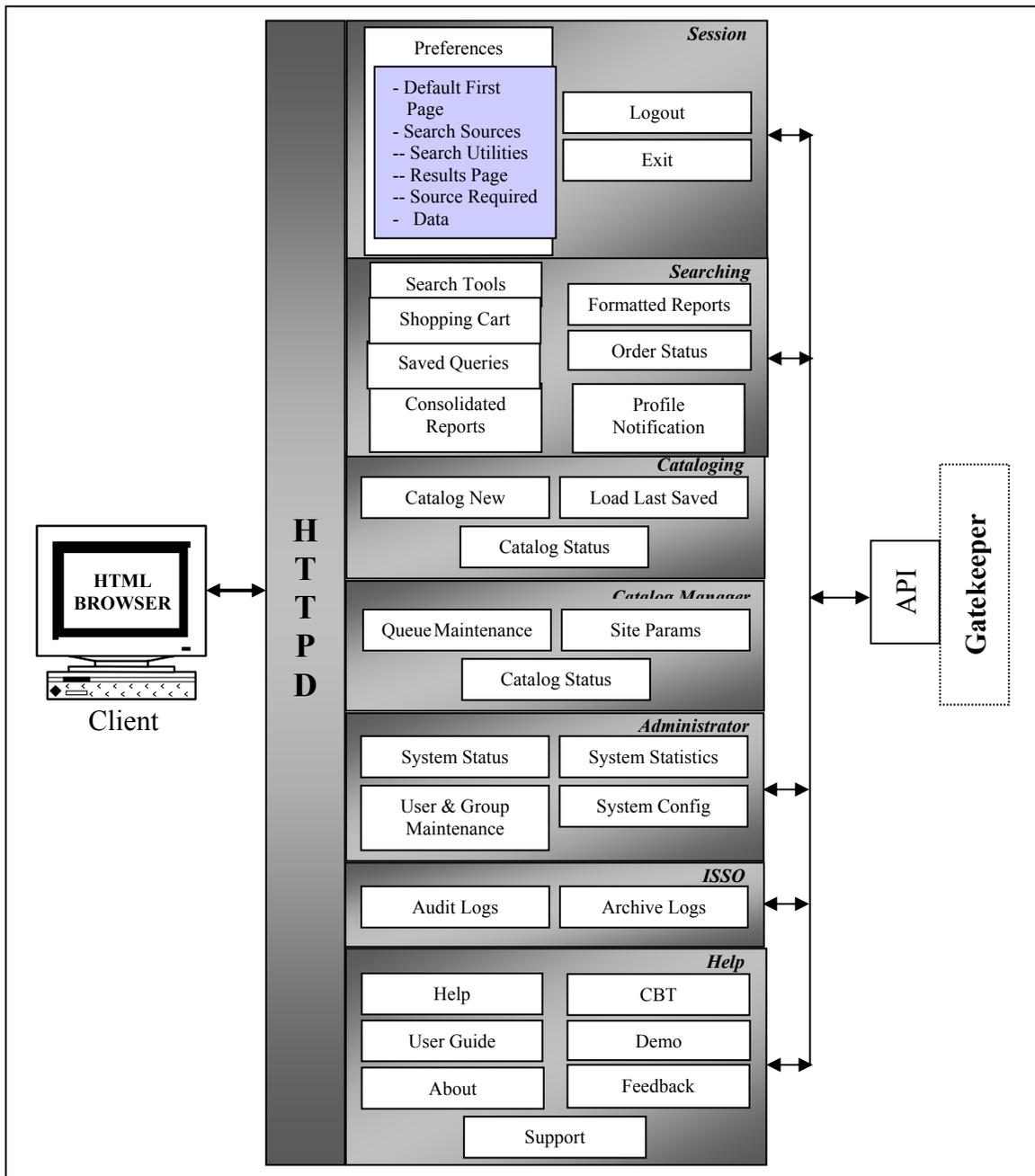


Figure 1.6 – User Interface Architecture

**1.3.5.1 General**

These Session and Help functions are available to all users.

**1.3.5.1.1 Session Menu**

FINAL

The Session menu allows the user to log off or exit Broadsword safely. Additionally, the Preferences section allows the user to set up their default values and is split into five separate pages: (1) Default First Page, (2) Search Sources, (3) Search Utilities, (4) Results Page and (5) Source Required Data. Users are able to define what their Search Tools page looks like, which data sources to search, and their preferred search mechanism.

### **1.3.5.1.2 Help Menu**

The Help menu offers much assistance to the user. The Help page offers context-sensitive assistance with Broadsword functionality. The Demo page takes the user through an animated and narrated example of how to use the specific functionality that they currently have loaded. The CBT is a full computer-based training application. The User Guide provides detail on all of Broadsword's General and Catalog functionality. The Feedback page allows the user to provide on-line suggestions and comments about the interface to the local Broadsword Administrator. The Support page provides a list of points of contact for requirements, the Broadsword help desk, local site system administration, site ISSO, and site Intelink officer. The About page provides the version number of the system, and to whom the current version is registered.

### **1.3.5.2 Searching**

Under searching, the user is provided with tools to discover, navigate, and retrieve information across various sources. Searching capability is given to all authenticated users.

Users are able to choose between an SQL form-based utility (Query) or a spatial tool (Geographic Search). In addition, users are able to combine these search tools and configure which method they prefer through the Session -> Preferences -> Search Utility page. This preference represents the search mechanism which will be displayed. Should the user select Search Tools as their default first page (through the Session -> Preferences -> Default First Page functionality), then this search mechanism will be displayed immediately after login. Thus the Search Tools page is a single user-selected page, tailored to each user's preference.

Provided off the spatial tool is the ability to turn on broadcast feeds (e.g., TRAP/TRE and/or MTI). The user can use these feeds for tip-off of potential activity within a given Area of Responsibility (AOR) and request additional available information of the area through the request mechanism.

The results are provided back in an aggregated view based on the requested item(s). The results window is then used as a portal to the metadata associated with the various results, as well as error-checking information on the status of the request. These results can be displayed as a sorted or unsorted list, as a timeline, or on a map. From the Results Page, the records can be further examined, products pulled, or products ordered. Frequently used queries may be saved using the Search Tools page. Each source dictates the display and/or retrieval of its products.

UNCLASSIFIED

FINAL

Currently Broadsword supports ordering CSIL, IPL, and 5D products. There are different processes for pulling IPL/5D products to a destination or ordering CSIL products. Users are able to choose several products of different types and put them into a “shopping cart”. The ordering attributes for any product placed in the cart can be modified while in the cart. Items placed in the cart can be saved from session to session and across multiple queries. At any time the user can order the items in the cart by clicking the order button. The user can find out the status of any orders that they have placed by clicking on the Order Status capability. This function provides information as to whether the product has been successfully delivered or has been shipped out (depending on the source).

Formatted reports provide the ability for the user to generate a set of predefined reports. Specific report types and the attributes available to generate them are based on the source and type. Reports can be ordered to a specified destination or available on-line.

The ‘Consolidated reports’ functionality provides the ability for the user to generate a series of predefined reports against one or more datasources of the same type. This has been implemented for the ALIA effort – Automated Logistics Information into the AOC.

The Saved Queries page provides the user with a list of all queries that the user saved on the Search Tools Page, as well as functionality to process the queries in different ways. A saved query can be used interactively by the user, producing immediate results, as well as by background processing, producing deferred results. Interactive use of saved queries includes immediate execution of the query, or loading the query for display and/or modification. Background processing of saved queries is done by the Update and Batched Query Profiles. Update Profiles periodically informs the user of new and updated products that match the saved query. Batched Query Processing allows the user to schedule the query to be executed at a later time. The results generated by these background processing utilities are viewed through the Profile Notification Page. Profile Notification capability not only allows viewing of Update and Batched results, but also deletion of these results. For viewing, the standard display format is used to present product information.

### **1.3.5.3 Cataloging**

Cataloging provides the user with the ability to catalog products to any IPL system that is connected to the local Gatekeeper. There are several cataloging utilities provided by the interface: Catalog New Product, Load Last Saved, and Catalog Status. The Catalog New Product page starts the process allowing the user to catalog product(s) into one or more IPL datasources. The Load Last Saved page allows the user to recall the most recent catalog session that was either cataloged or terminated due to time-out by the client. New with this version is the ability for the user to view the product that is enclosed with the meta-data. Clicking on the product link will pull the product to view as is to assure that the product and meta-data correlate to each other. The Catalog Status page shows the user the status of previously cataloged products.

FINAL

With Broadsword 3.1, there are additions to the Cataloging functionality. There are now two ways to generate products for ingestion into the IPL datasource(s) the Broadsword administrator has given the user catalog access to: Producer or Managed Producer. The Producer role is unchanged. The Managed Producer role has two differences: At the beginning of the cataloging process, the Managed Producer may does not have to add a username and password to their Session -> Preferences -> Source Required Data page. The Catalog Manager 's username and password are used when the product is sent to the IPL datasource. Additionally, the Managed Producer does not actually place the product(s) generated into the IPL. Instead, the products are placed into a managed queue for a Catalog Manager to review and deny, modify, and/or approve for cataloging. Any modifications made to a product by the Catalog Manager are reported in the Managed Producer's Catalog Status.

#### **1.3.5.4 Catalog Manager**

The Catalog Manager functionality is new to Broadsword version 3.1. The catalog manager(s) are responsible for reviewing managed and/or public queues for products and approving, denying, and/or modifying these products for cataloging into the local IPL datasource(s). They are able to check on the status of products they have approved, modified or denied. Additionally, they have the ability to edit the Site Validation rules that will be applied to the products by creating data lists, establishing mandatory elements or mandatory tables beyond the validation rules established by the source.

#### **1.3.5.5 Administration**

The System Administration (SA) section for the Gatekeeper provides system status, user/group maintenance, system statistics, and system configuration. System Status provides the status of all processes associated with Broadsword, the ability to turn on debug flags, and maintenance for Broadsword log files.

Under User & Group Maintenance, the SA grants additional privileges (e.g., Producer, Managed Producer, Catalog Manager, Administrator, and/or ISSO) and access to various datasources. System Statistics provides Web, Gatekeeper and Batched Profile statistics. Web statistics is based on Web Usage and provides such information as the amount of bytes transferred, the top number of pages accessed, and the total number of accesses. Gatekeeper statistics include a listing of the top 10 frequently accessed products and the 10 most frequently issued queries.

The System Configuration section allows the SA to modify or change the configuration information of the Gatekeeper, configure/edit/remove datasources, define values for attributes (used for popdowns as part of the Short Query form), and establish connectivity with other Gatekeepers through registration with the Keymaster.

FINAL

### 1.3.5.6 ISSO

The ISSO Interface provides the ability to view, archive, or remove audit information from the Broadsword Sybase Database based on user(s), date/time, and audit event. It also allows the ISSO to retrieve previously archived audits.

For the Administrator's Users Guide, see Attachment I

For the ISSO Users Guide, see Attachment II

## 1.4 Product Trademark Registration

*List the appropriate trademark notations; i.e., "Microsoft (MS) Windows New Technology (Windows NT®) operating system and other Microsoft™ products referenced herein are registered trademarks of Microsoft Corporation in the United States and other countries."*

Sybase, Inc. – Copyright © 1991, 1993 Sybase, Inc. All rights reserved. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in FARS subparagraphs 52-227-19(a)-(d) for civilian agency contracts and DFARS 252-227-7013(c)(1)(ii) for Department of Defense contracts. Sybase reserves all unpublished rights under the copyright laws of the United States. Sybase, Inc. 6475 Cristie Avenue, Emeryville, CA 94608, USA

The Apache Software Foundation – The Apache Software License, Version 11. Copyright © 2000 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear. 4. The names "apache" and "apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org). 5. Products derived from this software may not be called "Apache", nor may "apache" appear in the name, without prior written permission of the Apache Software Foundation. THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

UNCLASSIFIED

FINAL

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org>. Portions of this software are based upon public domain software originally written at the National Center for Supercomputer Applications, University of Illinois, Urbana-Champaign.

James Clark – The contents of this file are subject to the Mozilla public License version 1.0 (the “license”); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/MPL/> Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the license for the specific language governing rights and limitations under the License. The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright © 1998 James Clark. All Rights Reserved.

Cold Spring Harbor Lab – Written by Tom Boutell, 5/94. Copyright 1994, Cold Spring Harbor Labs. Permission granted to use this code in any fashion provided that this notice is retained and any alternations are labeled as such. It is requested, but not required, that you share extensions to this module with us so that we can incorporate them into new versions.

Digital Equipment Corporation – “Copyright 1990 Digital Equipment Corporation, Maynard, Massachusetts. All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Digital not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. DIGITAL DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OR MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL DIGITAL BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OF PERFORMANCE OF THIS SOFTWARE.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. Preamble The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to

UNCLASSIFIED

FINAL

share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow. GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION 0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does. 1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other

UNCLASSIFIED

FINAL

recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee. 2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License. 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code

UNCLASSIFIED

FINAL

means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code. 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance. 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it. 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License. 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This

UNCLASSIFIED

FINAL

section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License. 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License. 9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation. 10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally. NO WARRANTY 11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. 12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GTE – Copyright © 1994 GTE Government System Corporation Unpublished – all rights reserved under the copyright laws of the United States. The development of this

UNCLASSIFIED

FINAL

software was privately funded. As such, it falls within the provisions of DFARS 227.402-70 and 227-403-70. This software is delivered to the U.S. Government with restricted rights under the provisions of DFARS 252.227-7013.

Hewlett Packard Company, Silicon Graphics Computer Systems, Inc, Moscow Center for SPARC Technology, and Boris Fomitchev – Copyright 1994, Hewlett-Packard Company. Copyright © 1996, 1997, Silicon Graphics Computer Systems, Inc. Copyright © 1997, Moscow Center for SPARC Technology. Copyright © 1999 Boris Fomitchev.

Internet Software Consortium & IBM – Copyright © 1996, 1998 by Internet Software Consortium. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. Portions Copyright © 1995 by International Business Machines, Inc. International Business Machines (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission.

INTERSOLV, Inc & Microsoft Corp. – Copyright: 1992-1997 INTERSOLV, Inc. This software contains confidential and proprietary information of INTERSOLV, Inc. © Copyright 1990-1998 By Microsoft Corp.

David Koblas – Copyright 1990, 1991, 1993, David Koblas (koblas@netcom.com). Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided “as is” without express or implied warranty.

Thomas Lane, L Peter Deutsch – The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided “AS IS”, and you, its user, assume the entire risk as to its quality and accuracy. This software is copyright © 1991-1996, Thomas G. Lane. All Rights Reserved except as specified below. Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions (1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation. (2) If only executable code is distributed, then the accompanying documentation must state that “this software is based in part on the work of the Independent JPEG Group”. (3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind. These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us. Permission is NOT granted for the use of any IJG author’s name or company name in advertising or publicity relating to this software or products derived from it. This

UNCLASSIFIED

FINAL

software may be referred to only as “the Independent JPEG Group’s software”. We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor. Ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sol proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. Ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.C is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do. The configuration script “configure” was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. It appears that the arithmetic coding option of the JPEG specs is covered by the patents owned by IBM, AT&T and Mitsubishi. Hence, arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code. WARNING: Unisys has begun to enforce their patent on LZW compression against GIF encoders and decoders. You will need a license from Unisys to use the included rdgif.c or wrgif.c files in a commercial or shareware application. At this time, Unisys is not enforcing their patent against freeware, so distribution of this package remains legal. However, we intend to remove GIF support from the IJG package as soon as a suitable replacement format becomes reasonably popular. We are required to state that “The Graphics Interchange Format © is the Copyright property of CompuServe Incorporated. GIF (sm) is a Service Mark property of CompuServe Incorporated.

Ben Laurie – Copyright © 1995,6,7 Ben Laurie. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product include software developed by Ben Laurie for use in the Apache-SSL HTTP server project.” 4. The name “Apache-SSL Server” must not be used to endorse or promote products derived from this software without prior written permission. 5. Redistributions of any form whatsoever must retain the following acknowledgement : “This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.” THIS SOFTWARE IS PROVIDED BY BEN LAURIE “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AR DISCLAIMED. IN NO EVENT SHALL BEN LAURIE OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

UNCLASSIFIED

FINAL

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of patches to the Apache HTTP server interfacing it to SSLey. For more information on Apache-SSL; contact Ben Laurie <ben@algroup.co.uk>. For more information on Apache see [HTTP://www.apache.org/](http://www.apache.org/) or more information on SSLey see <http://www.psy.uq.oz.au/~ftp/Crypto/>.

Sam Leffler & Silicon Graphics, Inc. Copyright © 1998, 1989, 1990, 1991, 1992, 1993, 1994 Sam Leffler. Copyright © 1991, 1992, 1993, 1994, Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (1) the above copyright notices and this permission notice appear all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

Mark of the Unicorn, Inc – Copyright © 1997, Mark of the Unicorn, Inc. Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Mark of the Unicorn makes no representations about the suitability of this software for any particular purpose.

Stephen L Moshier – Cephes Math Library Release 2.3 – June, 1995. Copyright 1984, 1989, 1995 by Stephen L Moshier.

Northrup Grumman Surveillance and Battle Management Systems – Author: John Thaden COMPANY: Northrup Grumman Surveillance and Battle Management Systems. COPYRIGHT © 1999. All rights reserved.

OpenLDAP Foundation – Copyright 1998, 1999 the OpenLDAP Foundation, Redwood City, California, USA. All rights reserved. Redistribution and use in source and binary forms are permitted only as authorized by the OpenLDAP Public license. A copy of this license is available at <http://www.OpenLDAP.org/license.html> or in the file LICENSE in the top-level directory of the distribution.

Optivision, Incorporated – © Copyright 1988-1994, Optivision Incorporated. All rights are reserved. Copying or other reproduction of this program except for archival purposes is prohibited without the prior written consent of Optivision Incorporated, 1477 Drew Avenue, Suite 102, Davis California 95616.

Jef Poskanzer – Copyright © 1988 by Jef Poskanzer. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provide “as is” without express or implied warranty.

UNCLASSIFIED

FINAL

Promula Development Corporation – Copyright 1988 Promula Development Corporation. ALL RIGHTS RESERVED.

The Regents of the University of California – Copyright © 1989 the Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such.

RSA Data Security, Inc – Copyright © 1991-1992, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or reverencing this software or its function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

Richard M Stallman – Ghostscript General Public License (Clarified 11 Feb 1988)  
Copyright © 1988 Richard M Stallman. Everyone is permitted to copy and distribute verbatim copies of this license, but changing it is not allowed. You can also use this wording to make the terms for other programs. The license agreements of most software companies keep you at the mercy of those companies. By contrast, our general public license is intended to give everyone the right to share Ghostscript. To make sure that you get the rights we want you to have, we need to make restrictions that forbid anyone to deny you these rights or ask you to surrender the rights. Hence this license agreement. Specifically, we want to make sure that you have the right to give away copies of Ghostscript, that you receive source code or else can get it if you want it, that you can change Ghostscript or use pieces of it in new free programs, and that you know you can do these things. To make sure that everyone has such rights, we have to forbid you to deprive anyone else of these rights. For example, if you distribute copies of Ghostscript, you must give the recipients all the rights that you have. You must make sure they, too, receive or can get the source code. And you must tell them their rights. Also, for our own protection, we must make certain that everyone finds out that there is no warranty for Ghostscript. If Ghostscript is modified by someone else and passed on, we want its recipients to know that what they have is not what we distributed, so that any problems introduced by others will not reflect on our reputation. Therefore we (Richard M. Stallman and the Free Software Foundation, Inc.) make the following terms which say what you must do to be allowed to distribute or change Ghostscript. COPYING POLICIES 1. You may copy and distribute verbatim copies of Ghostscript source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy a valid copyright and license notice “Copyright © 1989 Aladdin Enterprises. All rights reserved. Distributed by Free Software Foundation, Inc.” (or with whatever year is appropriate); keep intact the notices on all files that refer to this License Agreement and to the absence of any warranty,; and give any other

UNCLASSIFIED

FINAL

recipients of the Ghostscript program a copy of this License Agreement along with the program. You may charge a distribution fee for the physical act of transferring a copy. 2. You may modify your copy or copies of Ghostscript or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following: a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and b) cause the whole of any work that you distribute or publish, that in whole or in part contains or is a derivative of Ghostscript or any part thereof, to be licensed at no charge to all third parties on terms identical to those contained in this license agreement (except that you may choose to grant more extensive warranty protection to some or all third parties, at your option). C) You may charge a distribution fee for the physical act of transferring a copy and you may at your option offer warranty protection in exchange for a fee. Mere aggregation of another unrelated program with this program (or its derivative) on a volume of a storage or distribution medium does not bring the other program under the scope of these terms. 3. You may copy and distribute Ghostscript (or a portion or derivative of it, under paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following: a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above, or b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal shipping charge) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above, or c) accompany it with the information you received as to where the corresponding source code may be obtained (this alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone. ) For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs 4. You may not copy, sublicense, distribute, or transfer Ghostscript except as expressly provided under this License Agreement. Any attempt to otherwise copy sublicense, distribute or transfer Ghostscript is void and your rights to use the program under this License Agreement shall be automatically terminated. However, parties who have received computer software programs from you with this License Agreement will not have their licenses terminated so long as such parties remain in full compliance. 5. If you wish to incorporate parts of Ghostscript into other free programs whose distribution conditions are different, write to the Free Software Foundation at 675 Mass Ave, Cambridge, MA 02139. We have not yet worked out a simple rule that can be stated here, but we will often permit this. We will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software. Your comments and suggestions about our licensing policies and our software are welcome! Please contact the Free Software Foundation, Inc at the above address or call (617) 876-3296. NO WARRANTY BECAUSE GHOSTSCRIPT IS LICENSED FREE OF CHARGE, WE PROVIDE ABSOLUTELY NO WARRANTY, TO THE EXTENT PERMITTED BY APPLICABLE STATE LAW, EXCEPT WHEN

UNCLASSIFIED

FINAL

OTHERWISE STATED IN WRITING, FREE SOFTWARE FOUNDATION, INC, RICHARD M STALLMAN, ALADDIN ENTERPRISES, L. PETER DEUTSCH AND/OR OTHER PARTIES PROVIDE GHOSTSCRIPT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF GHOSTSCRIPT IS WITH YOU. SHOULD GHOSTSCRIPT PROVE DEFECTIVE YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW WILL RICHARD M STALLMAN, THE FREE SOFTWARE FOUNDATION, INC., L. PETER DEUTSCH, ALADDIN ENTERPRISES, AND/OR ANY OTHER PARTY WHO MAY MODIFY AND REDISTRIBUTE GHOSTSCRIPT AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY LOST PROFITS, LOST MONIES, OR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE (INCLUDING BUT NOT LIMITED TO A LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS) Ghostscript, even if you have been advised of the possibility of such damages, or for any claim by any other party.

Sun Microsystems "Copyright © 1993 by Sun Microsystems, Inc. yaccpar 6.12"

Paul Vixie – Copyright © 1994-2000 World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. This program is distributed under the W3C's Software Intellectual Property License. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See W3C License <http://www.w3.org/Consortium/Legal/> for more details.

Frank Warmerdam – Copyright © 1999, Frank Warmerdam. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notices and this permission shall be included in all copies of substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNCLASSIFIED

FINAL

Eric Young – Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the colder is Tim Hudson (tjh@cryptsoft.com) Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at a program startup or in documentation (online or textual provided with the package).

## 1.5 References

*Provide a listing of directives, manuals, and other documents used as reference material. Include any security configuration guides used in the installation and secure configuration of the system.*

*Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems, 31 Mar 01*

*DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide, April 2001, DS-2610-142-01*

*Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, Revision 2, 31 March 2001*

*User Manual for the Air Force DoDIIS Infrastructure (AFDI) Unix Segment Version 1.1.0.1, Logicion-Sterling Federal, 2000*

*Common User Baseline for the Intelligence Community (CUBIC) Configuration Management Plan Version 3.0, August 2001*

*Broadsword 3.1 System Security Authorization Agreement, August 2002*

*Broadsword 3.1 System Installation Guide, August 2002*

UNCLASSIFIED

## 2 SYSTEM SECURITY OVERVIEW

### 2.1 System Environment

*Describe the organization(s) that the system supports and their location. Describe any security-specific components of the system architecture and the functions performed in addition to a high-level overall system architecture. Describe any network connections/interfaces. Document the classification of the data processed, the clearance level of the system's users, the Levels-of-Concern for Integrity and Availability and the Protection Level of the system. List the primary internal and external threats to the system and the countermeasures employed to mitigate them.*

<b>LOWEST CLEARANCE</b>	<b>FORMAL ACCESS APPROVAL</b>	Need To Know	Protection Level
At least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2
At Least Equal to Highest Data	NOT ALL Users Have ALL	Not Contributing to Decision	3
Secret	Not Contributing to Decision	Not Contributing to Decision	4
Uncleared	Not Contributing to Decision	Not Contributing to Decision	5

**Table 2.1 – Protection Levels**

Integrity Level-of-Concern is defined as the degree of resistance against unauthorized modification. Users granted access to sources connected within the Broadsword infrastructure are granted read-only privileges. Broadsword users can insert or modify any information on no source, except during IPL Production, which is regulated through discretionary access controls and the requirement of an IPL username and password. It has been determined that Broadsword shall meet a “MEDIUM” Level-of-Concern for Integrity.

Available Level-of-Concern defines the degree to which the system ensures that information is available for use, when, where, and in the form commensurate with the user's requirements. It has been determined that Broadsword shall meet a “MEDIUM” Level-of-Concern for Availability.

### 2.2 System and Security Management Roles and Responsibilities

*At a minimum, define the roles and responsibilities with respect to the secure operation of the system for the following individuals: Information System Security Manager (ISSM), Information System Security Officer (ISSO), Network Security Manager, Network Security Officer, System Administrator, Computer Operators, Privileged User, Non-Privileged User.*

<b>Role</b>	<b>Responsibility</b>
Information System Security Manager	<ul style="list-style-type: none"> <li>• Forwarding a copy of his/her appointment letter to the DAA Rep/SCO.</li> <li>• Developing and maintaining a formal IS security program.</li> <li>• Implementing and enforcing IS security policies.</li> <li>• Reviewing and endorsing all IS accreditation/certification support documentation packages</li> <li>• Overseeing all ISSOs to ensure they follow established IS policies and procedures.</li> <li>• Ensuring ISSM/ISSO review weekly bulletins and advisories that impact security of site information systems to include AFCERT, ACERT, NAVCIRT, IAVA, and DISA ASSIST bulletins.</li> <li>• Ensuring that periodic testing (monthly for PL5 systems) is conducted to evaluate the security posture of the IS's by employing various intrusion/attack detection and monitoring tools (shared responsibility with ISSOs).</li> <li>• Ensuring that all ISSOs receive the necessary technical (e.g., operating system, networking, security management, Sys Admin) and security training (e.g., ND-225 or equivalent) to carry out their duties.</li> <li>• Assisting ISSOs to ensure proper decisions are made concerning the levels of concern for confidentiality, integrity, and availability of the data, and the protection levels for confidentiality for the system.</li> <li>• Ensuring the development of system accreditation/certification documentation by reviewing and endorsing such documentation and recommending action to the DAA Rep/SCO.</li> <li>• Ensuring approved procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output.</li> <li>• Maintaining, as required by the DAA Rep/SCO, a repository for all system accreditation/certification documentation and modifications.</li> <li>• Coordinating IS security inspections, tests, and reviews.</li> <li>• Investigating and reporting (to the DAA/DAA Rep/SCO and local management) security violations and incidents, as appropriate.</li> <li>• Ensuring proper protection and corrective measures have been taken when an IS incident or vulnerability has been discovered.</li> <li>• Ensuring data ownership and responsibilities are established for each IS, to include accountability, access and special handling requirements.</li> <li>• Ensuring development and implementation of an effective IS security education, training, and awareness program.</li> <li>• Ensuring development and implementation of procedures in accordance with configuration management (CM) policies and</li> </ul>

FINAL

	<p>practices for authorizing the use of hardware/software on an IS. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM/ISSO and appropriate approving authority prior to the change.</p> <ul style="list-style-type: none"> <li>• Developing procedures for responding to security incidents, and for investigating and reporting (to the DAA Rep/SCO and to local management) security violations and incidents, as appropriate.</li> <li>• Serving as a member of the configuration management board, where one exists (however, the ISSM may elect to delegate this responsibility to the ISSO.)</li> <li>• Working knowledge of system functions, security policies, technical security safeguards, and operational security measures.</li> <li>• Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.</li> </ul>
<p>Information System Security Officer</p>	<ul style="list-style-type: none"> <li>• Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices as outlined in the accreditation/certification support documentation package.</li> <li>• Attending required technical (e.g., operating system, networking, security management, Sys Admin) and security (e.g., ND-225 or equivalent) training relative to assigned duties.</li> <li>• Ensuring all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.</li> <li>• Ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.</li> <li>• Reporting all security-related incidents to the ISSM.</li> <li>• Initiating protective and corrective measures when a security incident or vulnerability is discovered, with the approval of the ISSM.</li> <li>• Developing and maintaining an accreditation/certification support documentation package for system(s) for which they are responsible.</li> <li>• Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package.</li> <li>• Ensuring Configuration Management (CM) for IS software and hardware, to include IS warning banners, is maintained and documented.</li> <li>• Serving as member of the Configuration Management Board if so designated by the ISSM.</li> <li>• Ensuring warning banners are placed on all monitors and appear when a user accesses a system.</li> <li>• Ensuring system recovery processes are monitored and that</li> </ul>

UNCLASSIFIED

FINAL

	<p>security features and procedures are properly restored.</p> <ul style="list-style-type: none"> <li>• Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.</li> <li>• Formally notifying the ISSM and the DAA Rep/SCO when a system no longer processes classified information.</li> <li>• Formally notifying the ISSM and the DAA Rep/SCO when changes occur that might affect accreditation/certification.</li> <li>• Ensuring system security requirements are addressed during all phases of the system life cycle.</li> <li>• Following procedures developed by the ISSM, in accordance with configuration management (CM) policies and practices, for authorizing software use prior to its implementation on a system. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM and appropriate approving authority prior to the change.</li> <li>• Establishing audit trails and ensuring their review.</li> <li>• Administering user identification (USERID) and authentication mechanisms of the IS or network.</li> <li>• Ensuring the most feasible security safeguards and features are implemented for the IS or network.</li> <li>• Ensuring no attempt is made to strain or test security mechanisms, or perform network line monitoring, or keystroke monitoring without appropriate authorization.</li> <li>• Performing network monitoring for the purpose of identifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority.</li> <li>• Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.</li> </ul>
Network Security Manager	The Network Security Manager is a role defined by DIA and the site in conjunction.
Network Security Officer	The Network Security Officer is a role defined by DIA and the site in conjunction.
System Administrator	<ul style="list-style-type: none"> <li>• Implementing the IS Security guidance and policies as provided by the ISSM/ISSO.</li> <li>• Maintaining IS and networks to include all hardware and software (COTs/GOTs).</li> <li>• Monitoring system performance ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored.</li> <li>• Reporting all security-related incidents to the ISSM/ISSO.</li> <li>• Ensuring that all users have the requisite security clearances, authorization, need-to-know, and are aware of their security</li> </ul>

UNCLASSIFIED

FINAL

	<p>responsibilities before granting access to the IS.</p> <ul style="list-style-type: none"><li>• Performing equipment custodian duties by providing other system unique requirements that may be necessary. Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the accreditation/certification support documentation package.</li><li>• Maintaining software licenses and documentation.</li><li>• Notifying the ISSM/ISSO and the SCO formally when changes occur that might affect accreditation/certification.</li><li>• Ensuring Configuration Management (CM) for security-relevant IS software and hardware, to include IS warning banners, is maintained and documented.</li><li>• Monitoring hardware and software maintenance contracts.</li><li>• Establishing user identification (USERID) and authentication mechanisms of the IS or network and issue user logon identifications and passwords.</li><li>• Ensuring adequate network connectivity by ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.</li><li>• Establishing audit trails and conducting reviews and archives as directed by the ISSM/ISSO.</li><li>• Providing backup of system operations.</li><li>• Assisting the ISSM/ISSO in developing and maintaining accreditation/certification support documentation package for system(s) for which they are responsible.</li><li>• Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package.</li><li>• Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.</li><li>• Formally notifying the ISSM/ISSO and the SCO when a system no longer processes classified information.</li><li>• Following procedures developed by the ISSM/ISSO, authorizing software use before implementation on the system.</li><li>• Assisting the ISSM/ISSO in maintaining configuration control of the systems and applications software ensuring the most feasible security safeguards and features are implemented on the IS or network.</li><li>• Prohibiting attempts to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring without appropriate authorization.</li><li>• Performing network monitoring for the purpose of rectifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority and advising the ISSM/ISSO of security anomalies or integrity loopholes.</li></ul>
--	---

UNCLASSIFIED

FINAL

	<ul style="list-style-type: none"> <li>• Participating in the Information Systems Security incident reporting program and with the approval of the ISSM/ISSO, initiate protective or corrective measures when a security incident or vulnerability is discovered.</li> </ul>
Computer Operators	Computer Operators are covered under one or more of these other headings. They accumulate responsibilities with each role added.
Privileged User	<p>There are several different privileges available through the Broadsword software. These include the privileges to access datasources beyond those offered to the general user, which are assigned according to site policy regarding need-to-know and are covered by the rights and responsibilities as described under Non-Privileged User, below.</p> <p>Additionally, there are five roles available through the Broadsword interface which have varying degrees of privilege associated with them. These roles are Administration, ISSO, Producer, Managed Producer, and Catalog Manager.</p> <p>The Administration privilege is given to the privileged user(s) who will be maintaining the Broadsword server and software. It assists the users with the System Administration role (listed above) in completing their required functions. Therefore, the privileged users with the Administration privilege are addressed under the System Administration role description, above.</p> <p>The ISSO privilege is given to the privileged user(s) who match the Information System Security Officer role, listed above. The functionality granted by this role allows the ISSO to complete their required functions. Therefore, the privileged users with the ISSO privilege are addressed under the Information System Security Officer role description, above.</p> <p>The Producer role is given to the privileged user(s) who have permission to catalog products directly to a specific local IPL datasource. Rights and responsibilities beyond those of the Non-Privileged User include:</p> <ul style="list-style-type: none"> <li>* Ensure authenticity and correctness of products.</li> <li>* Follow site-specific production guidance.</li> </ul> <p>Note that these are in addition to the rights and responsibilities of the Non-Privileged User.</p> <p>The Managed Producer role is given to the privileged user(s) who have permission to populate a catalog queue for a specific local IPL datasource. Rights and responsibilities beyond those of the Non-Privileged User include:</p> <ul style="list-style-type: none"> <li>* Ensure authenticity and correctness of products.</li> </ul>

UNCLASSIFIED

FINAL

	<p>* Follow site-specific production guidance. Note that these are in addition to the rights and responsibilities of the Non-Privileged User.</p> <p>The Catalog Manager role is given to the privileged user(s) who have permission to review, approve, deny, or modify products contained in a catalog queue for a specific local IPL datasource. Rights and responsibilities beyond those of the Non-Privileged User include:</p> <ul style="list-style-type: none"> <li>* Ensure authenticity and correctness of products.</li> <li>* Follow site-specific production guidance.</li> </ul> <p>Note that these are in addition to the rights and responsibilities of the Non-Privileged User.</p>
<p>Non-Privileged User</p>	<p>The Non-Privileged, or "General", user of Broadsword</p> <ul style="list-style-type: none"> <li>* Follow the IS Security guidance and policies as provided by the ISSM/ISSO.</li> <li>* Report all security-related incidents to the ISSM/ISSO.</li> <li>* Make no attempts to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring.</li> <li>* Make no attempts to gain privileges beyond those assigned to them by the System Administrator, or in any other way attempting to compromise the system.</li> </ul>

**Table 2.2 – Role Definitions**

### **2.3 System User Access Policy**

This section describes each category of user and their access to system data and resources. The following is provided as a guide to help record the necessary information, but may be reformatted to suite the IS being described.

#### **2.3.1 User Access Controls**

*Discuss all system user access controls (e.g., log-on ID, authenticators, file protections).*

All user access controls are based upon a login ID and password. When the user logs into the system, the user is granted access to roles and data sources based upon this login ID. All of these accesses (including the act of logging in) are audited.

#### **2.3.2 Assignment and Control of Authenticators**

*Discuss procedures for assignment and control of authenticators.*

To create a Broadsword account, the system administrator needs to create a UNIX level account on the Broadsword server for the user. All password maintenance is performed at this level. If a user's account is locked, if its password is changed, or if it is deleted, this is automatically reflected in Broadsword. Broadsword Discretionary Access Controls are

UNCLASSIFIED

FINAL

modified by a Broadsword administrator through the Broadsword client. The procedures for assignment and control of authenticators are a site responsibility.

*If Passwords are used to control access, complete section 2.3.3 through 2.3.8.*

**2.3.3 IS User Access**

*Check all boxes that apply to the passwords assigned to the IS Users.*

<input checked="" type="checkbox"/>	All users have their own unique userid and unique password
<input type="checkbox"/>	Some users share a userid and password (Explain below)
<input type="checkbox"/>	Some users share a password (Explain below)

**Table 2.3 – Information System User Access**

Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.3.4 Privileged User Access**

*Select only one level of access*

The privileged users have a unique userid and unique password at the	
<input checked="" type="checkbox"/>	User level of access
<input type="checkbox"/>	Superuser level of access

**Table 2.4 – Privileged User Access**

**2.3.5 Password Changes**

*Select one box only*

<input type="checkbox"/>	<b>PASSWORDS ARE NOT CHANGED</b>				
<input type="checkbox"/>	Users can change their passwords but are not forced to change their passwords on any timely basis. I.E., passwords are changed whenever the user feels it necessary to change his/her password.				
<input checked="" type="checkbox"/>	Users are forced to change their passwords every .... (check all that apply)				
	<input type="checkbox"/> Month	<input checked="" type="checkbox"/> 6 Months	<input type="checkbox"/> Year	<input type="checkbox"/> NEVER	<input type="checkbox"/> After Initial Login
	<input type="checkbox"/> Other (Specify)				

**Table 2.5 – Password Change Policy**

Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.3.6 Password Generation**

Select all boxes that apply to the passwords.

<input checked="" type="checkbox"/>	Passwords are generated by the user
<input type="checkbox"/>	Users are encouraged by the ISSO or System Administrator to use “Strong” passwords wherever possible
<input type="checkbox"/>	System software forces users to create “Strong” passwords.
<input type="checkbox"/>	Passwords are generated by an IS.
<input type="checkbox"/>	Passwords are provided by an access control manager

**Table 2.6 – Password Generation**

Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.3.7 Number of Allowed Login Attempts**

Select one box only.

If a user enters the wrong userid or password:	
<input type="checkbox"/>	A timeout interval is enforced
<input type="checkbox"/>	NOTHING happens. The user can try to login as many times as he or she wishes
<input checked="" type="checkbox"/>	Maximum number of attempts: 3

**Table 2.7 – Allowed Login Attempt Count**

Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.3.8 Account Logout**

Check all that apply

<b>IF A USER’S ACCOUNT IS LOCKED OUT DUE TO EXCESSIVE INVALID LOGON ATTEMPTS, WHO IS AUTHORIZED TO REINSTATE THE USER’S ACCOUNT?</b>	
<input checked="" type="checkbox"/>	<b>SYSTEM ADMINISTRATOR</b>
<input type="checkbox"/>	ISSO
<input type="checkbox"/>	Superuser
<input type="checkbox"/>	Account Owner
<input type="checkbox"/>	System automatically reinstates the account after a specified time
<input checked="" type="checkbox"/>	Other (specify) : The site may have configured a CISSO user under the CSE-SS or AFDI applications which may be able to reinstate a user’s account.

**Table 2.8 – Account Logout**

Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.4 User Groups and Access Rights**

FINAL

**2.4.1 User Groups**

Check all boxes that apply to the procedures followed to assign access rights to users and administrators

<input type="checkbox"/>	Users and administrators are NOT assigned to groups; all userids are at the same level
<input type="checkbox"/>	All groups have the same privileges/access rights; users have the same access rights as administrators.
<input type="checkbox"/>	All administrators are assigned to a superuser group; the superuser group is different than the group(s) for users.
<input type="checkbox"/>	All users are assigned to the same group. This group has fewer privileges/access rights than the privileged user group.
<input type="checkbox"/>	Users are assigned to different groups depending on need-to-know and work assignments.
<input type="checkbox"/>	User groups have different privileges/access rights depending on need-to-know and work assignments.
<input checked="" type="checkbox"/>	Other: Broadsword uses the term "group" in three different contexts: Unix-level groups, Access Roles, and Groups of Users with similar need-to-know. All Broadsword users need to belong to the Unix-level "bswd" group to access certain functionality of the interface due to file permissions. Access Roles (such as General User, Administrator, or ISSO) are assigned on a user-by-user basis as determined by the site's policies. Finally, to reduce the administrative overhead, the Broadsword interface allows the Broadsword administrator to set up a 'group' of users that have identical permissions. These groups of users are designed and designated for users with identical need-to-know and usage requirements, and it is up to the local Broadsword Administrator to follow site policy to determine need-to-know.

**Table 2.9 – User Groups**

**2.4.2 System Files**

<input checked="" type="checkbox"/>	Users CANNOT change the configuration and/or content of system files.
<input type="checkbox"/>	Users can change the configuration and/or content of system files.

**Table 2.10 – System Files**

**2.4.3 System Access Rights**

<input type="checkbox"/>	Users CANNOT set the system access rights of other users.
<input checked="" type="checkbox"/>	Users can set the system access rights of other users (Describe).

**Table 2.11 – System Access Rights**

Administrative users have the ability to change other user roles (Administrator, IISO, and/or Producer). Additionally, administrators can set Discretionary Access Controls (DAC) to site data sources, allowing or denying access, as appropriate by a user's need-to-know. In addition, Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

**2.4.4 Audit Log Access**

<input type="checkbox"/>	Users CANNOT view, change, or delete the audit log.
<input checked="" type="checkbox"/>	Users can view the audit log.
<input checked="" type="checkbox"/>	Users can change or delete the audit log.

**Table 2.12 – Audit Log Access**

Users with the ISSO role only have the ability to review, archive, and delete audit records, and the ISSO role is a privileged role that must be granted to specific user(s). In addition, Broadsword is accredited based on the secure configuration of the system, as described in the Broadsword Install Guide. Any modifications to these configurations may void that accreditation.

#### **2.4.5 Privileged Users**

*Identify the number of privileged users and the criteria used to determine privileged access.*

All users have the ability to search data sources (though the sources available for search are based upon the individuals need-to-know, as defined by the discretionary access controls). Additionally, users may have access to one or more of the following privileged roles: Producer, Administrator, or ISSO.

Broadsword Producers, Managed Producers, and Catalog managers have varying degrees of ability to catalog new imagery into local IPL servers. This role is granted on a source by source basis (i.e. - a producer does not necessarily have the ability to catalog products into all of the site's IPLs).

Broadsword Administrators have the ability to configure new data sources, to set discretionary access controls on these sources, and to set other configuration information about the system. Additionally, the administrator has access to system statistics collected by the system, certain status and log files, and utilities to set other user roles and source access permissions.

Broadsword ISSO users have the ability to generate, review, archive and delete audit records.

The number of privileged users, and the criteria used to determine who has these privileges, is completely determined by the local site's policy.

#### **2.4.6 DAC/MAC**

*If DAC or MAC is required, discuss those mechanisms that implement the DAC and MAC controls.*

The Broadsword Administrator has the ability to restrict source access through DAC. When a source is created, if the source does not allow access by default, then the administrator has to manually add access to that source. Access can be added for a particular user, or to a group of users.

FINAL

### **3 SECURITY RELATED FEATURES AND PROCEDURES**

Describe the security features of the system and detailed information about the who, what, when, where, why and how of each feature with respect to mitigating risk to the system. Describe the security operating procedures for the system with respect to users, roles, and responsibilities. Topics to be addressed may include:

- System startup and shutdown procedures and order (include servers, workstations, and other components, as applicable)
- Audit event definition and management
- Event log definition and management
- Audit reduction, review, and analysis
- Audit log archive and restore procedures
- Time synchronization
- Operating system updates
- Application updates
- Removable media handling procedures
- Anti-virus tasks
- Account management
- System and network management
- System security policy maintenance
- User groups and roles management
- Access Control List management

The following set of instructions may be used to begin recording the necessary information. All security-related topics and procedures should be included.

#### **3.1 Protection of the Security Support Structure.**

Hardware and Firmware protections are a site responsibility. Broadsword software has file permission protections on the binary and configuration files. It further protects the server by limiting the protocols to the server (i.e., tftp, rlogin, rshell are not available).

#### **3.2 Security Features and Assurances.**

##### **3.2.1 Incident Reporting**

SITE POLICY

##### **3.2.2 Remote Access**

Broadsword implements SSL between the web browser and the web server to provide a replay attack resistant path for users to remotely access the system.

UNCLASSIFIED

FINAL

### 3.2.3 Change Control

SITE POLICY

### 3.2.4 Configuration Management

Broadsword is developed and maintained under a six-month spiral development process. The software is maintained by AFRL/IFE under the Common User Baseline for the Intelligence Community (CUBIC) Configuration Management (CM) Program. User conferences are conducted every six months. These conferences allow users to share their issues with the current release, see the version in development and to identify new requirements. Based on the outcome of the conference, the future releases are refined. All PRs and CRs are maintained on-line using the Configuration Management Data Base (CMDB).

All hardware change control is the responsibility of the site.

### 3.2.5 Security Features

*Discuss any security features unique to the system*

#### 3.2.5.1 Secure Socket Layer (SSL)

To provide additional layers of security, Broadsword v3.1 has implemented SSL. Broadsword provides SSL at 3 different points: 1) Between the user's web browser and the Broadsword Web server, 2) Between the Gatekeeper and Keymaster, and 3) between the Local and Remote Gatekeepers. Adding SSL protection at these 3 connections provides greater protection against both external and internal threats.

### 3.2.6 System Startup

To restart Broadsword:

```
% su - root
# /opt/bswd3.1/scripts/startserver
(answer Y, Y to the startserver prompts)
```

**Example 3.1 – System Startup**

### 3.2.7 System Shutdown

To safely stop Broadsword:

UNCLASSIFIED

```
% su - root
# /opt/bswd3.1/scripts/stopservers
  (if the dataserver is shared (e.g. - co-located on an IPL server) answer N N Y Y to the
  prompts, otherwise answer Y Y.)
```

### 3.3 Auditing

#### 3.3.1 User-level Auditing

Discuss the auditing procedures used to monitor user access and operation of the system and the information that is to be recorded in the audit trail. State whether audit trails of user access are manual or automatic.

##### 3.3.1.1 Querying the System for Audits

The ISSO Interface provides the ability to view, archive, or remove audit information from the Broadsword Sybase Database based on each of the following criteria:

Parameter	Description
User:	The user account being queried for audit information. DEFAULT: Blank; indicates all user accounts are being queried for audit information.
Start Date:	The start date/time of the audit information being queried. DEFAULT: Current date/time NOTE: if Start Date and End Date are identical, the system will be queried across all time.
End Date:	The end date/time of the audit information being queried. DEFAULT: Current date/time NOTE: if Start Date and End Date are identical, the system will be queried across all time.
Event:	The audit event being queried. POSSIBLE ENTRIES: All Events, Added DAC, Added Group, Added Group Member, Removed Group, Removed Group Member, Added New Source, Get Column Attributes, Added User Privileges, Audit Dump, Get Audit Archive List, Delete Audit, Gatekeeper Started, Gatekeeper Stopped, Got Audit Report, Modified Element, Query, Remove DAC, Remove Source, Remove Remote Gatekeeper, Remove User Privileges, Set Source Parameter, Set User DAC, Transfer Request, Catalog Request, User Logged In, User Logged Out, Clear Statistics, Accept Registration From Remote Gatekeepers, Register Our Gatekeeper With Keymaster, Update Daemon Status, New or Updated Gatekeeper Info, Initiate Stream Request, Terminate Stream Request, Client Profile Management, Client Profile Queue Management
Archive File Name:	Name of file to contain audit records being archived. (The directory path is <i>not</i> included in the filename.) PURPOSE: Needed only when using the "Archive Records" feature.

Table 3.1 – Audit Query Parameters

## FINAL

**3.3.1.2 Understanding the Audits**

The Broadsword components work together to provide the ISSO with a comprehensive set of tools for a) identifying who has accessed what information and b) assisting in the identification of significant security events. Specific audits logged by each of the components are provided in the following sections. Since Broadsword is a distributed architecture, it is important for the ISSO to understand where the information to answer a specific question exists. This section examples of all of the Gatekeeper audits that can be generated by user actions in the Broadsword client. The audits are broken up into three categories:

**(1) User and Producer Audits**

- Logging into the Gatekeeper
- Performing Queries on Local Sources
- Performing Product Requests on Local Sources
- Cataloging a Product
- Logging out of the Gatekeeper
- An Example with Local and Remote Requests

**(2) Administrative Audits - Configuring and Maintaining the System**

- Gatekeeper Maintenance
- INK Maintenance
- Global Registration/Maintenance
- User Maintenance
- Group Maintenance
- Operations Maintenance

**(3) ISSO Audits****3.3.1.3 User and Producer Audits**

To begin, user launches a web browser on their local workstation and types in the URL of the assigned Gatekeeper (a Gatekeeper which they have a login and password). The Broadsword system returns the home page for that Gatekeeper which requests that the user types in their login and password. Once the user has clicked the Accept button, the audit trail begins.

Table 3.2 provides a summary of the possible audits collected during a session for a user who is neither an Administrator nor an ISSO. In the following sections we will provide samples for each of the audits and conclude this section with a sample user session.

User Security Audits		
EVENT DESCRIPTION	Event Name	Configuration
User Logged In	LOGIN	All
Query	QUERY	All
Transfer Request	REQUEST	All
Catalog Request	CATALOG	All
Initiate Stream Request	INITSTREAM	All
Terminate Stream Request	TERMINATESTREAM	All
Client Profile Management		Not Used By Client
Client Profile Queue Management		Not Used By Client
Get Column Attributes	ATTRIBUTES	All
User Logged Out	LOGOUT	All

Table 3.2 – List of User Audits

### 3.3.1.3.1 Logging into the Gatekeeper

The first audit record that is cut for any user (regardless of what function or roles they have) is the initiation of a session. When a user logs into or attempts to log into the Gatekeeper, an audit record is cut. To generate a report of user logins the ISSO can either request All Events or select only User Logged In under the Event popup list. Selecting All Events will display the entire log to include login, queries, results, and product pulls. Selecting only User Logged In will provide only a list of login attempts.

The login audit record contains two lines. The first provides the user login, the IP Address of the machine they are logging in from, the user's ID on that workstation, the Gatekeeper's IP Address they are logging into and a unique session identifier. The session identifier will be unique for each time the user is logged in. The second line of Example 3.2a shows a successful log in.

```

Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user
Gtkpr: 123.45.678.89 Session Key: 4907

LOGIN: @ 20000926105608: Successful Login from Daleth
Gatekeeper
    
```

Example 3.2a - Sample Login Record (Successful Login)

Example 3.2b shows the audit that is cut when either an invalid login or password is entered.

## FINAL

```
Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user
Gtkpr: 123.45.678.89 Session Key: 4907
```

```
LOGIN: @ 20000926105608: Invalid Login from Daleth
Gatekeeper
```

**Example 3.2b - Sample Login Record (Invalid Login)**

The user has a number of times in which they must correctly enter the login and password. If they do not, the account will be automatically disabled. Example 3.2c displays the audit record identifying that the account was disabled. Prior to this record would be a number of invalid login audit records (as shown in Example 3.2b).

```
Login: gen_user IP: 123.45.678.90 Orig. Login: gen_user
Gtkpr: 123.45.678.89 Session Key: 4907
```

```
LOGIN: @ 20000926105608: Login disabled from Daleth
Gatekeeper
```

**Example 3.2c - Sample Login Record (Login Disabled)****3.3.1.3.2 Performing Queries on Local Sources**

There are many capabilities provided to the user once they have logged in. Most of the features of the client are for personalization and do not require auditing. From a security viewpoint, the majority of auditable events can be put into two categories: (1) queries or requests and (2) product pulls or deliveries. Queries or requests are presented to the Gatekeeper through its application programmers interface (API), are audited by the Gatekeeper, and routed to the appropriated plugin(s). For each source that the user has queried an audit record is written verifying that the request was sent to the plugin and is being processed. The plugin then processes the request and sends the translated request to the source itself. When the source responds, the plugin processes the results and passes them back to the Gatekeeper, who in turn writes an audit record identifying the specific items returned as a result of the request and the total number of hits.

To generate a report of queries the ISSO can either request All Events or select only Query under the Event popup list. Example 3.3 provides a sample query/response set of audits. The first audit provides a summary of the request. This includes the type of query (simultaneous or sequential), whether thumbnails were requested, the maximum number of hits requested, the request itself and the source(s). The second line provides a list of the hits returned and a total of the number returned.

UNCLASSIFIED

## FINAL

```
QUERY @ 20000926105608 : Query Accepted, QUERY
TYPE=SIMULTANEOUS, THUMBNAIIS=Y, MAX_HITS=5(0=ALL),
BQS=IMG.SOURCE="TEST" from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327205627650 from 5D at
Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970327211927560 from 5D at
Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827081558206 from 5D at
Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827082616003 from 5D at
Titan via Daleth
QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED08002021976808002021976819970827083055386 from 5D at
Titan via Daleth
QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth
```

**Example 3.3 - Sample Query/Response Record****3.3.1.3.3 Performing Product Requests on Local Sources**

Depending on the type of source, there are two possible mechanisms to pull a product through the Broadsword Client: (1) Pull to View and (2) Deliver to Destination(s). From the Gatekeeper's viewpoint both mechanisms are the same - the only difference being the destination directory. Once the imagery product is in the desired format and compression, the product is delivered to the specified destination(s). In the case of a "pull to view," the product is delivered into a directory so that the client can set the content type and stream the file to the browser. If the request was a "deliver to destination(s)," the product will be delivered to the destination(s) and directory(s) specified by the user through FTP. The client sends the request to the Gatekeeper, which in turn audits the request, creates a status record into the status log and routes the request through the plugin. The plugin, in turn, routes the request to the source.

To generate a report of product pulls the ISSO can either request All Events or select only Transfer Request under the Event popup list. Example 3.4 below shows the events generated whenever a user requests a product.

UNCLASSIFIED

## FINAL

```

REQUEST @ 20000926105854 : Request Accepted from 5D at
Titan via Daleth

REQUEST @ 20000926105910 :
26105854ZSep00.000095134512128123177001000010000004907
ACCESSID: FIVED08002021976808002021976819970827081558206
FORMAT: (ASIS) DEST IP ADDRESS: 123.45.678.89 DESTLOGIN:
bswdreg DESTPATH:
/opt/bswd3.1/client/PROTECTED/docs/session/4906/ FILENAME:
bswdreg.FIVED08002021976808002021976819980897081558206.NITF
02.00 STATUS: Transfer successful. from 5D at Titan via
Daleth

```

**Example 3.4 - Sample Product Request/Delivery**

The first line of the request record identifies that the request was passed on to the source. The second line provides a unique identifier for the request (the last five characters will contain the user's session id), the specific product that was requested, the format, the IP Address of the delivery destination, its directory and file name. It also provides the status of the delivery.

**3.3.1.3.4 Cataloging a Product**

The Broadsword Interface also allows users to produce imagery into IPL datasources. Every time a producer sends a product to the IPL's input queue, an audit record is generated.

To generate a report of cataloged products the ISSO can either request All Events or select only Catalog Request under the Event popup list. Example 3.5 shows a product being sent to the IPL 2.5.1 at Saturn with the title of "BSWD PEND TEST LPA0."

```

CATALOG @ 20001005151630 : Catalog New Product Accepted,
PRODUCT TITLE: BSWD PEND TEST LPA0 from IPL 2.5.1 at Saturn

CATALOG @ 20001005151630 : Catalog New Product Ftp to
IPA/IPL Successful. PRODUCT TITLE: BSWD PEND TEST LPA0
from IPL 2.5.1 at Saturn

```

**Example 3.5 - Catalog a new product into IPL 2.5.1**

The first record identifies that the IPL 2.5.1 plugin has accepted the product. The second record indicates that the plugin initiated an FTP session with the appropriate IPL 2.5.1 and that it was successful. At this point there is no way to find out whether the product

UNCLASSIFIED

## FINAL

was successfully ingested into the IPL database. IPL itself does not provide back any status.

### 3.3.1.3.5 Logging out of the Gatekeeper

The last audit that is possible during a user session, is the logout record. Upon successful logout, an audit record is written identifying that the session was terminated. To generate a report of user logouts the ISSO can either request All Events or select only User Logged Out under the Event popup list. Example 3.5a provides a sample of this audit.

```
LOGOUT @ 20000926110202 : Connection closed from daleth  
Gatekeeper
```

#### Example 3.5a - Logout Record

The Broadsword system implements a dead man timeout. Since the Broadsword client uses a Web browser, it is possible for it to terminate abnormally or for the user to exit the browser without logging out. In either of these cases, the session process will stay around. To allow for a graceful termination of these unconnected processes and to provide these resources back to the system, a timeout has been implemented. If there is an extended period of inactivity in a user's session (default is 30 minutes) the session will be terminated automatically. On those occasions a different logout audit record will be written (refer to Example 3.5b).

```
LOGOUT @ 20000926110202 : Gatekeeper timed out from daleth  
Gatekeeper
```

#### Example 3.5b - Logout Record (user timed out)

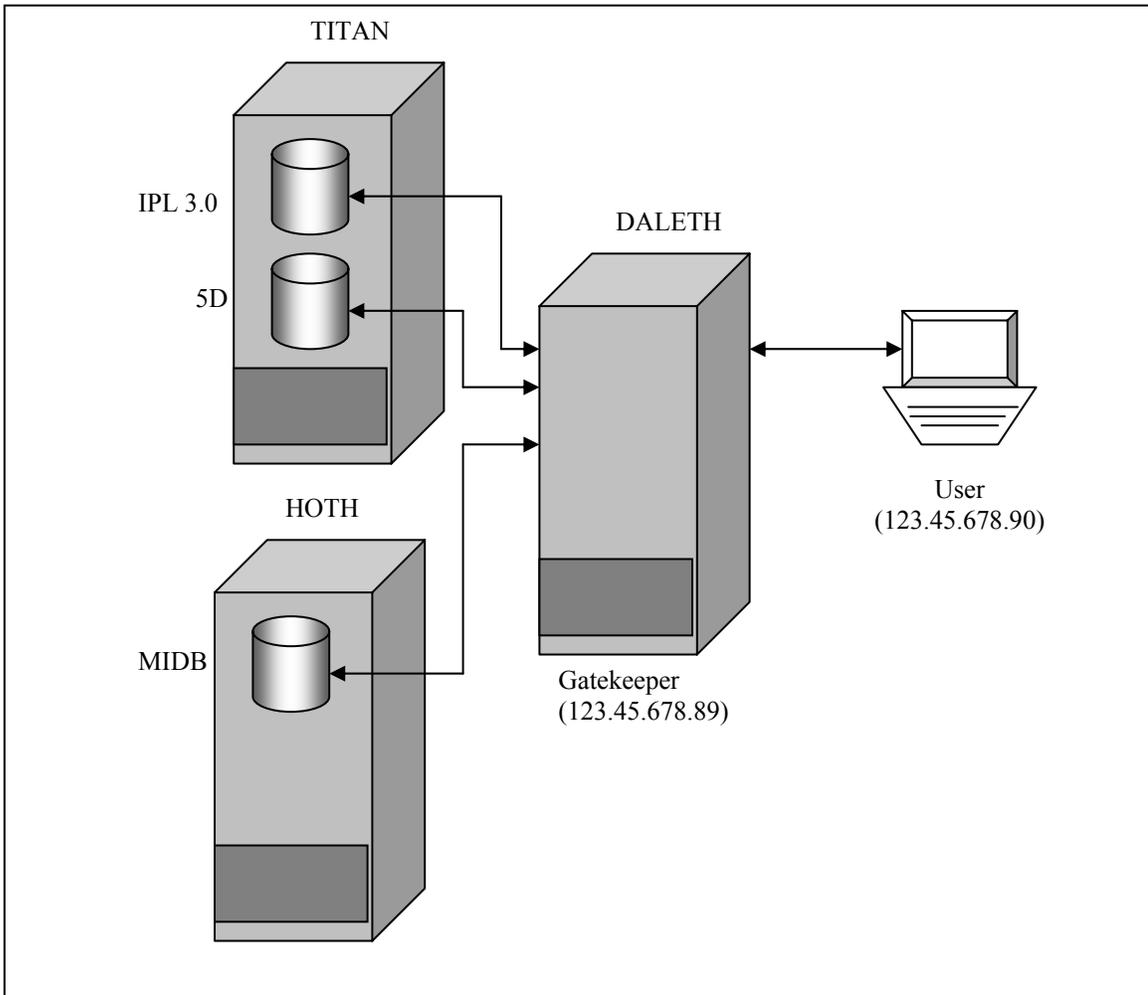
### 3.3.1.4 Putting It All Together

In this next section we provide two audit reports. The first contains only local requests, while the second has both local and remote.

#### 3.3.1.4.1 An Example with Only Local Requests

Our first example, as pictured in Figure 3.1, includes only one Gatekeeper. A Gatekeeper (Daleth, IP Address 123.45.678.89) is connected to three local sources: IPL 1.0, 5D and MIDB. The IPL 1.0 and 5D reside on the same server (Titan) while the MIDB resides on a second server (Hoth). The name of the MIDB has been augmented by its version name, Othello. For our example, the user workstation is using the IP Address 123.45.678.90 and the username "gen\_user."

UNCLASSIFIED



**Figure 3.1 Performing a Local Request**

To view what the user has done, the ISSO would go to the Audit Log Maintenance page under the ISSO menu. This capability allows the ISSO to query the audit database. To continue with our example, the ISSO would enter the user name, "gen\_user" and click on the Audit Report button. The Gatekeeper processes the request and an audit report will be generated. To view the report, the ISSO will next click on the "View Audit Report" anchor located in the middle of the page. Figure 3.2 provides an example audit report.

## Audit Report

User: gen\_user For All Dates For All Events.

Login: gen\_user IP: 123.45.678.90 Orig. Login: gen\_user  
Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Successful Login from Daleth  
Gatekeeper

QUERY @ 20000926105608 : Query Accepted, QUERY  
TYPE=SIMULTANEOUS, THUMBNAIIS=Y,  
MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Titan  
via Daleth

QUERY @ 20000926105608 : Query Accepted QUERY  
TYPE=SIMULTANEOUS, THUMBNAIIS=Y,  
MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from IPL 3.0 at  
Titan via Daleth

QUERY @ 20000926105608 : Query Accepted QUERY  
TYPE=SIMULTANEOUS, THUMBNAIIS=Y,  
MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from MIDB Othello  
at Hoth via Daleth

QUERY @ 20000926105619 : Unsupported Query Element:  
IMG.SOURCE for MIDB Othello at Hoth via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327205627650 from 5D at  
Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327211927560 from 5D at  
Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827081558206 from 5D at  
Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827082616003 from 5D at  
Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827083055386 from 5D at  
Titan via Daleth

QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth

QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED80201de96719970826204727486 from IPL 3.0 at Titan via  
Daleth

FINAL

```
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204522533 from IPL 3.0 at Titan via
Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204301083 from IPL 3.0 at Titan via
Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826204109470 from IPL 3.0 at Titan via
Daleth
QUERY @ 20000926105619 : GKPR 123.45.678.89, PRD.ACCESSID:
FIVED80201de96719970826203915123 from IPL 3.0 at Titan via
Daleth
QUERY @ 20000926105619 : 5 Hits from IPL 3.0 at Titan via
Daleth

LOGOUT @ 20000926110202 : Connection closed from daleth
Gatekeeper
```

**Figure 3.2 - Sample Audit Report (Request) for User "gen\_user"**

FINAL

### 3.3.1.4.2 Interpreting the Audits

The first line of the audit record indicates the beginning of a session. The Login identifies the user name of the person logged in. The IP is the IP address of the machine that the user has connected from. The Orig. Login is the username of that the user logged into the workstation with (if this information can be resolved). Gkpr is the IP address of the Gatekeeper the user has logged into. Session Key is a unique session identifier.

The second line identifies at what time the user attempted to login, the status of that login (Successful) and the name of the Gatekeeper that the user has logged into (Daleth Gatekeeper). The next set of records indicates that the user has initiated a query. Each record identifies what source the user has queried, what the user has queried for, the type of query (simultaneous or sequential), the number of hits to be returned from the source and, if supported, whether thumbnails have been requested or not. In this example, the 5D at Titan, IPL 3.0 at Titan and MIDB at Hoth were queried for up to five hits where IMG.SOURCE="TEST". At this point the Gatekeeper passes the query to the appropriate plugins and waits for their responses.

As each plugin returns, it provides status back to the Gatekeeper. The first response is from the MIDB plugin. The query submitted for the MIDB contained an element not supported (IMG.SOURCE) by MIDB and was blocked by the plugin.

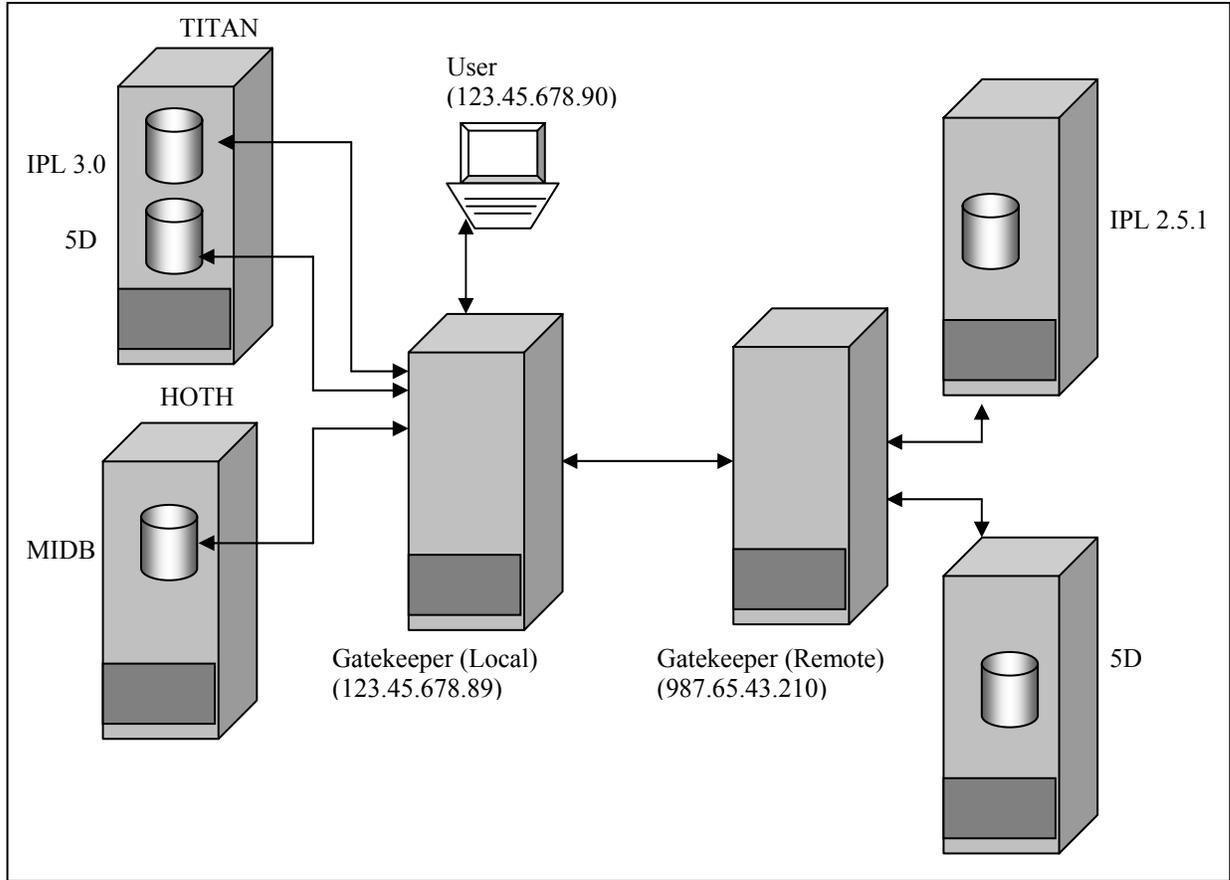
The next set is from the 5D. Each record is uniquely identified using the Product's Access ID (PRD.ACCESSID). The last line of this set identifies that 5 hits (the maximum requested) were returned.

The last set of records is from the IPL30 plugin. Like 5D, each hit returned from the IPL is uniquely identified using the Product's Access ID. The last line again identifies the number of hits returned from the IPL. In our example, the IPL returned 5 hits. Since the user/client requested a maximum of 5 hits, only 5 are sent back. The last line of our example is the log out record. It identifies when the user logged out and that the connection with the Gatekeeper has been closed.

### 3.3.1.4.3 An Example with Local and Remote Requests

Our next example, as pictured in Figure 3.3, builds upon the previous example. It includes both our local Gatekeeper and an additional remote Gatekeeper with its own sources. The remote Gatekeeper (Beth, IP Address 987.65.43.210) has connected to it two sources, 5D and IPL 2.5.1.

UNCLASSIFIED



**Figure 3.3 - Performing a Local & Remote Request**

The local Gatekeeper continues to keep track of all requests and responses made by its local users. When the ISSO generates an audit report for a specific user at the Gatekeeper to which the user has logged in, all user activities are contained at that Gatekeeper. Remote Gatekeepers will also contain audit information for that portion of the request that they are responsible for.

In our example, the ISSO responsible for the given user (i.e. the local Gatekeeper's ISSO), through a similar query as with the previous example, will generate a single report for the given user including all requests/results from both the local and remote sources. If the ISSO performs a similar request (through the ISSO interface) on the remote Gatekeeper, the report will contain only information pertaining to that Gatekeeper's sources. Figure 3.4 provides a sample of the reports generated from the local and remote Gatekeepers.

Reviewing the audit report, we see that the user logged in and queried a local 5D, a remote 5D, and a remote IPL 2.5.1. The request was sent to the respective sources, accepted and processed. The results were then returned and the user logged out.

### 3.3.1.4.3.1.1 Audit Report

User: gen\_user For All Dates For All Events.

Login: gen\_user IP: 123.45.678.90 Orig. Login: gen\_user Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULT ANEOUS, THUMBNAI LS=Y, MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Titan via Daleth

QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULT ANEOUS, THUMBNAI LS=Y

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULT ANEOUS, THUMBNAI LS=Y

-----  
Q: How do I know this includes a remote query?  
A: This is not the name of the local Gatekeeper.  
-----

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327205627650 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970327211927560 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827081558206 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827082616003 from 5D at Titan via Daleth

QUERY @ 20000926105617 : GKPR 123.45.678.89, PRD.ACCESSID:  
FIVED08002021976808002021976819970827083055386 from 5D at Titan via Daleth

QUERY @ 20000926105619 : 5 Hits from 5D at Titan via Daleth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826204727486 from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : Saturn IPA: 00001 Hit from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826204109470 from 5D at Neptune via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826203915123 from 5D at Neptune via Beth

QUERY @ 20000926105619 : Saturn IPA: 00003 Hits from 5D at Neptune via Beth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

### 3.3.1.4.3.1.2 Audit Report

User: gen\_user For All Dates For All Events.

Login: gen\_user IP: 123.45.678.90 Orig. Login: gen\_user Gtkpr: 123.45.678.89 Session Key: 4907  
LOGIN: @ 20000926105608: Successful Login from Daleth Gatekeeper

QUERY @ 20000926105608 : Query Accepted, QUERY TYPE=SIMULT ANEOUS, THUMBNAI LS=Y, MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from 5D at Saturn via Beth

QUERY @ 20000926105608 : Query Accepted QUERY TYPE=SIMULT ANEOUS, THUMBNAI LS=Y, MAX\_HITS=5(0=ALL),BQS=IMG.SOURCE="TEST" from IPL 2.1 at Neptune via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826204727486 from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : Saturn IPA: 00001 Hit from IPL 2.1 at Saturn via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826204301083 from 5D at Neptune via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826204109470 from 5D at Neptune via Beth

QUERY @ 20000926105619 : GKPR 987.65.43.210, PRD.ACCESSID:  
FIVED80201de96719970826203915123 from 5D at Neptune via Beth

QUERY @ 20000926105619 : Saturn IPA: 00003 Hits from 5D at Neptune via Beth

LOGOUT @ 20000926110202 : Connection closed from daleth Gatekeeper

FIGURE 3.4 - SAMPLE AUDIT SESSION WITH LOCAL & REMOTE QUERIES

### 3.3.1.4.4 Identifying Audit Anomalies

It is apparent, from reading the previous sections, that an audit report can contain extensive amounts of information. The question is what does the ISSO do with this information? What is the ISSO looking for? The ISSO is answering questions such as: Who is accessing the system? What is being accessed? Have there been any attempts to penetrate the system?

The last question is one that we are concerned with. The ISSO needs some way to identify that activity that might indicate attacks on the system. Such indicators can be invalid logins, bad MD5 seals, or unexpected system downtime. Broadsword provides an anomaly detection tool that allows an ISSO to easily identify malicious behavior.

The Broadsword Audit logs will highlight any audit records containing anomalous keywords, as demonstrated below.

```
Audit Report
User: test Starting at: 20010216175029 and Ending at : 20010316175029 For All
Events.

LOGIN: test IP: 100.200.300.400 Orig.Login NotATest Gtkpr: 100.200.300.401
Session Key: 54
LOGIN @ 20010219181326: Successful Login from saturn Gatekeeper for bswd
3.1
LOGOUT @ 20010219171722: Connection close from saturn Gatekeeper for
bswd 3.1
Login: test IP: 100.200.300.400 Orig.Login NotATest Gtkpr: 100.200.300.401
Session Key: 23104
LOGIN @ 20010316142716 : Successful Login from saturn Gatekeeper for bswd
3.1
QUERY @ 20010316143211 : Query Accepted, QUERY
TYPE=SIMULTANEOUS, THUMBNAILS=Y,MAX_HITS=10 (0=ALL),
BQS=TGT.CC="IZ" from IPL 2.5.1 at Ariel via SATURN LPA3 SDE
QUERY @ 20010316143127 Could Not Connect to IPL 2.5 Database from IPL
LOGOUT @ 20010316144102: Gatekeeper timed out from saturn Gatekeeper for
bswd3.1
```

Anomaly highlight

Figure 3.5 - Audit Report with Highlighted Anomaly

The ISSO may configure this utility by specifying new keywords and phrases to identify. To modify this list, the ISSO should edit the file

FINAL

/opt/bswd3.1/client/etc/audit\_anomalies.conf on the Broadsword server. This file contains keywords to search for, one per line. To add a new key phrase to search for, merely add a new line to the file. The search phrases are not case sensitive. Once the phrase has been added, save the file and exit. The change will be reflected immediately; no process needs to be stopped or restarted.

### 3.3.1.5 Administrative Audits - Configuring and Maintaining the System

The Broadsword client provides the Administrator the ability to (1) configure/tailor the Broadsword system to a site's specific needs, (2) maintain the system and (3) obtain system status and statistics. Chapters 7 and 8 describe these capabilities. The purpose of this section is to describe the audits that are generated when the administrator performs a given function. An administrator is allowed to change only the information/configuration of the Gatekeeper that they are logged into. Table 3.3 provides a summary of the audits generated by the administrator.

User Security Audits		
EVENT DESCRIPTION	Event Name	Configuration
<b>Gatekeeper Maintenance</b>		
Added New Source	CREATESRC	ALL
Set Source Parameter	SETSRCPARAM	ALL
Set User Discretionary Access Control (DAC)	SETUSERDAC	ALL
Added Discretionary Access Control(DAC)	ADDDAC	ALL
Remove Source	DELETESRC	ALL
Remove Discretionary Access Control (DAC)		Not Used By Client
<b>INK Maintenance</b>		
Modified Element	MODELEMENT	ALL
<b>Global Registration/Maintenance</b>		
Register Our Gatekeeper with Keymaster	REGOURGKPR	ALL
New or Updated Gatekeeper Info	CONFIGUPDATE	ALL
Update Daemon Status	UPDATE_DAEMON	ALL

UNCLASSIFIED

<b>User &amp; Group Maintenance</b>		
Added User Privileges	ADDUSER	ALL
Remove User Privileges	DELUSER	ALL
Added Group Member	ADDGROUPMEMBER	ALL
Removed Group Member	DELGROUPMEMBER	ALL
Added Group	ADDGROUP	ALL
Modified Group	MODGROUP	ALL
Removed Group	DELGROUP	ALL
<b>Operations</b>		
Gatekeeper Started	GATEKEEPER STARTED	ALL
Gatekeeper Stopped	GATEKEEPER SHUTDOWN	ALL
Clear Statistics		Not Used By Client

**Table 3.3 – List of Administrator Audits**

The audit events described below are examples of typical audit records generated by an administrator. The specific auditable events include adding backside sources, configuring attributes, modifying users and registering the gatekeeper with the Keymaster.

### **3.3.1.5.1 Gatekeeper Maintenance**

The administrator has the ability to add or modify a backside source. Shown below are three examples of sources being added. Each source requires a number of parameters to be filled in. These parameters vary from source to source. The three examples show the different accesses that can be granted to a source: No Access, Local Access Only, and Local & Remote Access.

When a source is configured with No Access, by default no users have access to the source. In order to allow access to such a source, the administrator needs to grant that user access (see Chapter 4). Sources set to allow Local Access Only allow access only to those users logged into the given Gatekeeper. If the Gatekeeper is registered with a Keymaster, then any sources set to allow Local & Remote Access will allow all local users to access the source, and will also allow all users on other Gatekeepers in the Keymaster's domain to access the source.

Example 3.6a shows the creation of a new backside source. The source that was added was an IPL 2.1 to the Gatekeeper on Daleth.

```
CREATESRC @ 20001004054446 : IPL21 Source Created with  
Reference of 8092cff8:970611035:IPL21:970616918 from Daleth  
Gatekeeper
```

```
SETSRCPARAM @ 20001004054842 : Following parameters Changed  
For IPL 2.1 at AFRL: Query Max Hits, IPL 2.1 Host IP  
Address, IPL 2.1 TCP/IP Port, IPL 2.1 Site Name, IPL Host  
IP Address, IPL Order Status Port, IPL 2.1 Account, IPL 2.1  
Sybase IP Address, IPL 2.1 Sybase Port, IPL21 Database  
Name, IPL 2.1 SQS Sybase Server IP Address, IPL 2.1 SQS  
Sybase Server Port, IPL 2.1 Database Login, Access  
Permission Override, IPL 2.1 Password, IPL 2.1 Database  
Password from Daleth Gatekeeper
```

```
SETUSERDAC @ 20001004054843 : ALL Allowed Access to IPL 2.1  
at AFRL from Daleth Gatekeeper
```

**Example 3.6a - Add an IPL 2.1 source and allow access to all users**

The CREATESRC record was generated by the creation of the source. The SETSRCPARAM record shows a list of all of the source parameters set when the source was created. The SETUSERDAC record is generated when the client sets the list of users allowed access to the source to ALL. Example 3.6b shows the creation of a new IPL 1.0 source that has been made available to only local users.

FINAL

```
CREATESRC @ 20001004054446 : IPL Source Created with  
Reference of 8092aae7f2:935556478:IPL:972337212 from Daleth  
Gatekeeper
```

```
SETSRCPARAM @ 20001004054842 : Following parameters Changed  
For IPL at AFRL: Query Max Hits, IPL Host IP Address, IPL  
TCP/IP Port, IPL Site Name, IPL Host IP Address, IPL Order  
Status Port, Harvest TCP/IP port, Format Conversion Flag,  
IPL Account, Access Permission Override from Daleth  
Gatekeeper
```

```
ADDDAC @ 20001004054843 : None Allowed Access to  
8092aae7f2:935556478:IPL:972337212 from Daleth Gatekeeper
```

```
SETUSERDAC @ 20001004054843 : 8092aae7f2:935556478 Allowed  
Access to IPL at AFRL from Daleth Gatekeeper
```

**Example 3.6b - Add an IPL 2.1 source and allow access to only local users**

In this example, the ADDDAC call is made to explicitly to allow no access to the source. Then the SETUSERDAC call adds 8092aae7f2:935556478 (Daleth's Gatekeeper Reference) to the access list. This allows all of Daleth's local users to access this source.

Example 3.6c shows the creation of a new 5D source that, by default, does not allow access to any users.

```
CREATESRC @ 20001004071517 : 5D Source Created with Reference of  
8092cff8:970611035:5D:970622117 from Daleth Gatekeeper
```

```
SETSRCPARAM @ 20001004071520 : Following parameters Changed  
For 5D at AFRL: Query Max Hits, Query Plugin Name, Request  
Plugin Name, 5D Sybase IP Address, 5D Sybase Port, 5D  
Database Name, 5D Catalog Directory, 5D Database  
Login, IPL TCP/IP Port, IPL Order Status Port, IPL 2.0  
Account, Access Permission Override from Daleth Gatekeeper
```

```
SETUSERDAC @ 20001004054843 : ALL Denied Access to 5D at  
AFRL from Daleth Gatekeeper
```

**Example 3.6c - Add a 5D source and deny access to all users**

In this example, the SETUSERDAC call is made to deny access to all users.

UNCLASSIFIED

## FINAL

There are two additional functions available for configuring sources. These are the modification of a parameter of a source and the removal of a source. Example 3.7 shows the audit record that is written when a source attribute has been modified while Example 3.8 is an audit record when the source has been removed.

```
SETSRCPARAM @ 20001101023601 : Following parameters Changed  
For John's IESS: Exploitation Sybase Port, Imagery_Coverage  
Sybase Port from saturn Gatekeeper
```

**Example 3.7 - Modification of a Source Parameter**

```
DELETESRC @ 20001004054843 : Source IPL21 (IPL 2.1 at AFRL)  
Deleted With Reference of  
8092cff8:970611035:IPL21:970616918 from Daleth Gatekeeper
```

**Example 3.8 - Removal of a Source (IPL 2.1 at AFRL)**

There are a number of system or gatekeeper parameters that were configured during the installation process. There may be a need to change this information. If any of this information is changed, it will be audited. Example 3.9 shows an audit record when the Point of Contact field was modified.

```
SETSRCPARAM @ 20001013113738 : Following parameters Changed  
for Daleth Gatekeeper: Point of Contact from Daleth  
Gatekeeper
```

**Example 3.9 - Modifying the Gatekeeper's Point of Contact****3.3.1.5.2 INK Maintenance**

Using the DE Configuration capability, the administrator can modify an existing attribute's name, help, and popdown values. Example 3.10 and Example 3.11 The following examples show the audits cut when the administrator has gone into the DE configuration page and selected the CLASS attribute under the PROD (Product) table. In Example 3.10 the administrator has removed an entry from the popdown list. In Example 3.11, the administrator has added a new entry to the popdown list.

UNCLASSIFIED

```
MODELEMENT @ 20001006114746 : Section PRD Element CLASS
Changes:
```

```
Display Name Data Help for Daleth Gatekeeper
```

```
MODELEMENT @ 20001006114748 : Section PRD Element CLASS
Changes: Deleting From Data List from Daleth Gatekeeper
```

**Example 3.10 - Modifying the Gatekeeper's Point of Contact**

```
MODELEMENT @ 20001006114746 : Section PRD Element CLASS
Changes:
```

```
Display Name Data Help for Daleth Gatekeeper
```

```
MODELEMENT @ 20001006114748 : Section PRD Element CLASS
Changes: Adding
```

```
To Data List Data List Help from Daleth Gatekeeper
```

**Example 3.11 - Adding a new popdown**

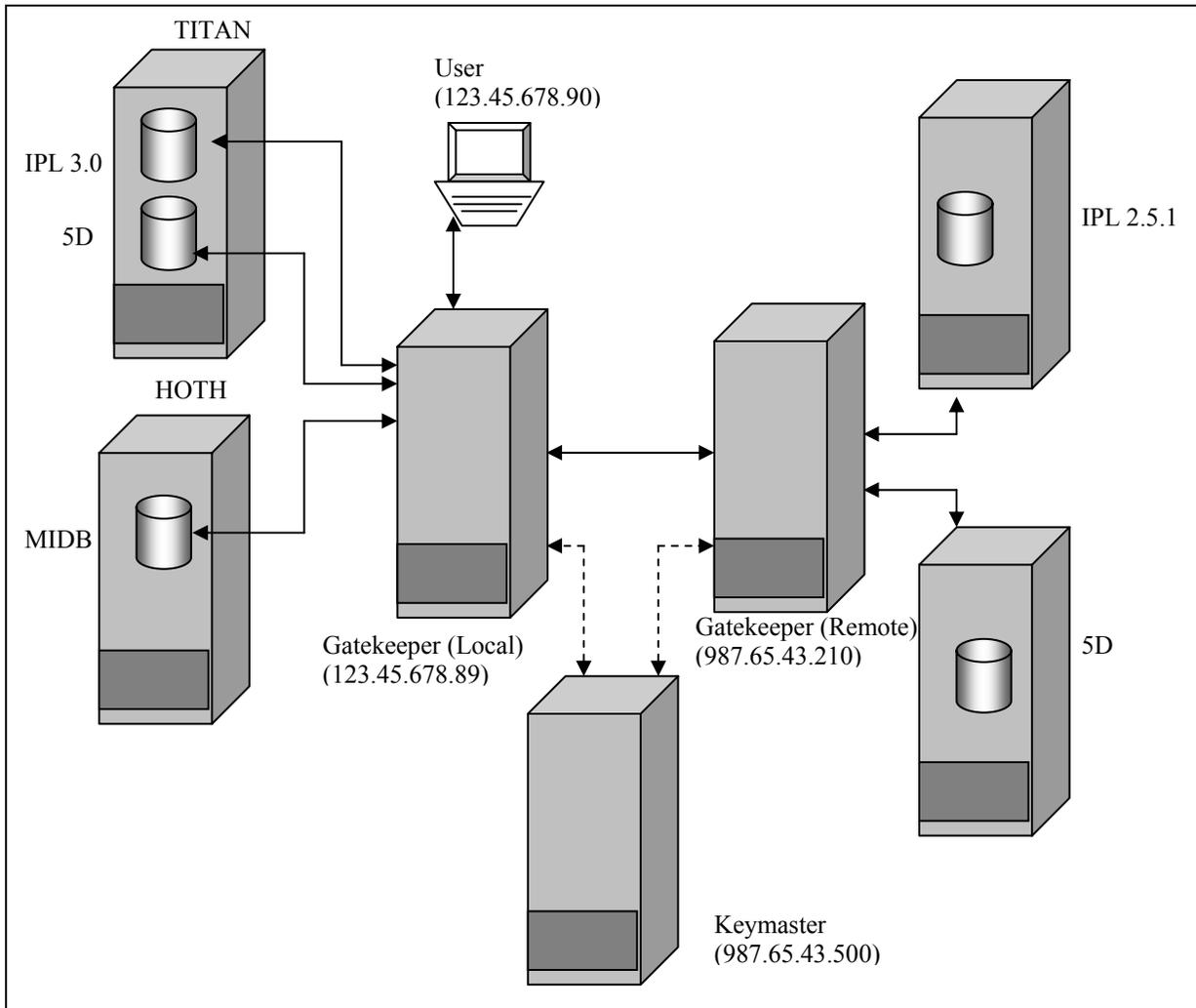
### 3.3.1.5.3 Global Registration/Maintenance

Broadsword v1.0 allowed a site to grant a single point of access to local data sources for all of the site's users. Broadsword v2.0 introduced the Keymaster. The Keymaster allows the creation of a virtual network between Gatekeepers. Each Gatekeeper has the ability to publish local data sources (this list is called the Gatekeeper's local map), thus allowing users at other sites to access these sources (recall Figures 3.6 and 3.7). The Keymaster maintains a global list of each Gatekeeper's local map (referred to as the global map). Table 3.4 provides a list of Keymaster audit events.

<b>Administrative Security Audits for Keymaster ONLY</b>	
<b>3.3.1.5.3.1.1.1.1 Event Description</b>	<b>Event Name</b>
Accept Registration from Remote Gatekeeper	INITREG
New or Updated Gatekeeper Info	CONFIGUPDATE
Update Daemon Status	UPDATE_DAEMON
Unregister Gatekeeper	UNREGGKPR

**Table 3.4 – Keymaster Audit Events**

Figure 3.6 shows the sample environment that we will consider for the following examples:



**Figure 3.6 – Sample Environment Configuration**

When a new Gatekeeper joins the network of Gatekeepers, it must first register itself with the Keymaster. The process begins when the system administrator of the new Gatekeeper calls the Keymaster Distribution Center. From the Keymaster administrator, a unique registration identifier will be generated for the new Gatekeeper. The system administrator of the new Gatekeeper will then enter this registration identifier, the port number of the Keymaster and the Keymaster's IP address into the Gatekeeper's registration screen. At this point the Gatekeeper will then generate a public/private key pair and send the Keymaster a message containing: (1) its public key, (2) the one time registration identifier and (3) a map identifying the sources to be made publicly available (set to Allow Local & Remote Access).

Once the Keymaster has processed the Gatekeeper's registration message, the Keymaster will respond with a message containing: (1) the Gatekeeper's digital certificate (a timestamp, the Gatekeeper's identification and the Gatekeepers public key) encrypted

FINAL

using the Keymaster's private key, (2) a second digital certificate describing the Keymaster, and (3) the world map of all other Gatekeepers and their publicly available (published) sources. The Keymaster will complete the registration process by alerting all other Gatekeepers to the existence of the new Gatekeeper. Once this is accomplished, a periodic background process checks for any map updates and, if necessary, sends each Gatekeeper a new map.

In some circumstances it becomes necessary to remove a Gatekeeper from a Keymaster's community. The Keymaster administrator has the ability to remove a Gatekeeper from the community. This removes all global map and certificates from the removed Gatekeeper, and removes all references to that Gatekeeper from the other Gatekeepers' maps.

Figures 3.7a and 3.7b provide example audit records from a successfully completed Gatekeeper registration, a map update, and the unregistration of a Gatekeeper.

### Gatekeeper Logs (daleth)

Login: bswduser IP: 123.45.678.90 Orig.Login  
bswduser Gtkpr: 123.45.678.89 Session Key 10484  
LOGIN @ 20001204184746 : Successful Login  
from daleth Gatekeeper  
REGOURGKPR @ 20001204184955 :  
Registration Successful, to Gkpr: 987.65.43.500,  
Port: 5700, Desc: io Keymaster from daleth  
Gatekeeper  
LOGOUT @ 20001204185207 : Connection  
closed from daleth Gatekeeper

Login: root IP: Orig. Login: Gtkpr: 987.65.43.500  
Session Key: 10672  
LOGIN @ 20001204184959 : Successful Login  
from io Keymaster  
LOGOUT @ 20001204185137 : Connect ion  
closed from io Keymaster  
CONFIGUPDATE @ 20001204185137 :  
Configuration Update From io Keymaster, IP  
Addr: 123.45.678.90 Was Successful from io  
Keymaster

**Unregister Gatekeeper**

**Map Updates**

### Keymaster Logs (io)

Login: keyadmin IP 987.65.43.500 Orig. Login:  
keyadmin Gtkpr: 987.65.43.500 Session Key 672  
LOGIN @ 20001204184358 : Successful Login  
from io Keymaster  
INITREG @ 20001204186438 : Gatekeeper  
Registration Started from io Keymaster  
INITREG @ 20001204184958 : Gatekeeper  
Registration Completed For daleth Gatekeeper  
from io Keymaster  
LOGOUT @ 20001204190507 : Connection  
closed from io Keymaster

Login: root IP: 987.65.43.500 Orig Login: root  
Gtkpr: 987.65.43.500 Session Key 813  
UPDATE\_DAEMON @ 20001204184957 :  
Update Daemon Started from io Keymaster  
UPDATE\_DAEMON @ 20001204185013 :  
Successfully sent Configuration To (beth  
Gatekeeper), with Ref (80aae5f1:987654123) from  
io Keymaster  
UPDATE\_DAEMON @ 20001204185013 :  
Successfully sent Configuration To (daleth  
Gatekeeper), with Ref (80bac5f4:982434109) from  
io Keymaster  
UPDATE\_DAEMON @ 20001204185138 :  
Update\_daemon Exiting from io Keymaster

**Figure 3.7a – Register a New Gatekeeper**

### Gatekeeper Logs (daleth)

Login: root IP: Orig.Login: Gtkpr: 987.65.43.500  
Session Key: 10672  
LOGIN @ 20001204184959 : Successful Login  
from io Keymaster  
LOGOUT @ 20001204185137 : Connection  
closed from io Keymaster  
CONFIGUPDATE @ 20001204185137 :  
Configuration Update From io Keymaster, IP  
Addr: 123.45.678.90 Was Successful from io  
Keymaster

**Unregister Gatekeeper**

**Map Updates**

### Keymaster Logs (io)

Login: keyadmin IP: 987.65.43.500 Orig. Login:  
keyadmin Gtkpr: 987.65.43.500 Session Key 8960  
LOGIN @ 20001205143551 : Successful Login  
from io Keymaster  
UNREGGKPR @ 20001205143551 : daleth  
Gatekeeper Unregistered With Reference of  
80bac5f4:982434109 from io Keymaster  
LOGOUT @ 20001205143851 : Connection  
closed from io Keymaster

Login: root IP 987.65.43.500 Orig. Login: root  
Gtkpr: 987.65.43.500 Session Key 813  
UPDATE\_DAEMON @ 20001204184957 :  
Update Daemon Started from io Keymaster  
UPDATE\_DAEMON @ 20001204185013 :  
Successfully sent Configuration to (beth  
Gatekeeper), with Ref (80aae5f1:987654123) from  
io Keymaster  
UPDATE\_DAEMON @ 20001204185013 :  
successfully sent Configuration to (daleth  
Gatekeeper) , with Ref (80bac5f4:982434109)  
from io Keymaster

Figure 3.7b – Unregistering a Gatekeeper

FINAL

**3.3.1.5.4 User Maintenance**

Broadsword version 3.1 supports the way in which user access and authentication was performed in version 2.0. The site will continue to create user accounts through CSE-SS or AFDI and add privileges/accesses through the Broadsword administration interface.

Existing users can be deleted. Only the user's Broadsword-related files are removed. The user still has a valid UNIX login. To completely remove the user from the system, his or her account must be removed through the tool used to create it. If the account is not removed, the user will still be capable of logging into the Broadsword client and have all the default sources and privileges. Example 3.12 displays the audit record that is written when a user account has been removed.

```
DELETEUSER @ 20001005150223 : gen_user Deleted As General
User from daleth Gatekeeper
```

**Example 3.12 - Removing an Existing User**

Once the administrator has created the account using CSE-SS/AFDI/Sun Tools, the administrator can add/remove sources, add privileges or roles, and add the user to a group.

For those sources that were configured to have the access flag set to Deny All, the administrator must individually grant a user access to those sources. When the administrator grants this access, an audit record (as shown in Example 3.13) is written.

```
SETUSERDAC @ 20001101025620 : gen_user Allowed Access to
IESS at AFRL from saturn Gatekeeper
```

**Example 3.13 - Adding Source Access for a User**

Likewise, when the administrator removes access to a given source an audit record (as shown in Example 3.14) is written.

```
SETUSERDAC @ 20001101025727 : gen_user Denied Access to
IESS at AFRL from saturn Gatekeeper
```

**Example 3.14 - Adding Source Access for a User**

The administrator can add additional privileges to a user account. These privileges include Administrator, ISSO, and producer/catalog ability. The example below shows that the user "gen\_user" was given the ability to catalog to an IPL 2.1 system.

```
ADDUSER @ 20001005150223 : gen_user Added To Producer List
for Reference 8092cff8:970611035:IPL21:970616918
```

UNCLASSIFIED

FINAL

**Example 3.15 - Adding Role Privilege**

```
DELETEUSER @ 20001101032917 : bswduser Deleted From  
Producer List For Reference  
80b40e1e:968967577:IPL:968969809 from saturn Gatekeeper
```

**Example 3.16 - Removing Role Privilege**

In addition to assigning privileges to an individual, the administrator can add the user to one or more groups that already have the appropriate privileges. The following examples show a user being added (Example 3.17) and removed (Example 3.18) from a group.

```
ADDGROUPMEMBER @ 20001101033851 : bswduser Added To Group  
Test from saturn Gatekeeper
```

**Example 3.17 - Adding a User to the Group 'Test'**

```
DELGROUPMEMBER @ 20001101034300 : bswduser Deleted From  
Group Test from saturn Gatekeeper
```

**Example 3.18 - Removing a User from the Group 'Test'**

### 3.3.1.5.5 Group Maintenance

Users can belong to one or more groups. Groups allow the administrator to group a set of common accesses and privileges together. By doing this, the administrator does not have to add roles and sources to each user individually. For example, if the site wishes to grant several users the ability to catalog to one or more IPLs, the administrator can create a group, (i.e. DBM with Description of Data Base Managers) and assign one or more producer roles to the group. They can then go under users (under groups) and simple move each user over to become a member of the group. Example 3.19 shows the audit record written when the group is created.

```
ADDGROUP @ 20001006120814 : Added Group DBM, Description:  
Data Base Manager from Daleth Gatekeeper
```

**Example 3.19 - Created Group Named 'DBM'**

Once the group has been created, sources, roles and users can be assigned. For each source added to the group a SETUSERDAC event will be written. This record will look similar to the SETUSERDAC when a source is added to a specific user. When the group is granted additional roles or privileges, an ADDUSER event record is written and likewise as each user is added to the group under group membership an ADDGROUPMEMBER audit record is written. Example 3.20 provides an example of the record that is written when the group description is changed.

UNCLASSIFIED

FINAL

MODGROUP @ 20001006120814 : Modified Group DBM,  
Description: Data Base Managers from Daleth Gatekeeper

**Example 3.20 - Modified Description for Group Named 'DBM'**

Example 3.21 provides an example of an audit record when a user is added to a group.

ADDGROUPMEMBER @ 20001006120814 : testact1 Added To Group DBM from Daleth Gatekeeper

**Example 3.21 - Added User Named 'testact1' to Group Named 'DBM'**

Example 3.22 provides an example of an audit record when a user is removed from a group.

DELGROUPMEMBER @ 20001228211835 : testact1 Deleted From Group DBM from Daleth Gatekeeper

**Example 3.22 - Deleted User Named 'testact1' to Group Named 'DBM'**

Example 3.23 provides an example of an audit record when the group is deleted.

DELGROUP @ 20001006120814 : Deleted Group DBM from Daleth Gatekeeper

**Example 3.23 - Deleted Group Named 'DBM'**

**3.3.1.5.6 Operations Maintenance**

Upon startup, the Gatekeeper cuts an audit record.

GATEKEEPER STARTUP @ 20001006120814 : Gatekeeper Server Startup Using Solaris BSM from daleth Gatekeeper

**Example 3.24 - Gatekeeper Startup**

**3.3.1.5.7 ISSO Audits**

All of the audits presented up to this point were retrieved through the ISSO interface in the Broadsword application. The ISSO can do more than just search the audit logs. The ISSO can also archive the audits to a file on the system, query these archives for specific events, and delete both these archives and the audit records. Each of these events is audited to provide full accountability. Table 3.5 provides a list of security audits that are generated in response to ISSO actions.

ISSO Security Audits		
Event Description	Event Name	Configuration
Audit Dump	DUMPAUDIT	All
Delete Audit	DELETEAUDIT	All
Got Audit Report	GETAUDITRPT	All

**Table 3.5 – ISSO Audits**

UNCLASSIFIED

Examples 3.25 - 3.28 give samples of the possible security audits that can be generated by an ISSO using the ISSO tools.

```
GETAUDITRPT @ 20001005100007 : Audit Report Generated for
User gen_user From Date 20001005085925 To Date
20001005095925 For Event QUERY from Daleth Gatekeeper
```

**Example 3.25 - Query Audit Records**

```
DUMPAUDIT @ 20001101034832 : Audit Report Dumped for User
gen_user To File johns_test from saturn Gatekeeper
```

**Example 3.26 - Generate an Audit Archive**

```
GETAUDITRPT @ 20001101035016 : Audit Report Generated From
Archive: File(s) johns_test from saturn Gatekeeper
```

**Example 3.27 - Query an Archive Record**

```
DELETEAUDIT @ 20001013113608: Audit Deleted for User
gen_user from Daleth Gatekeeper
```

**Example 3.28 - Delete an Audit Record**

Example 3.25 provides the audit record generated by an ISSO querying the audits. In this case, the query was for any queries performed by gen\_user over the last hour. In Example 3.26, the ISSO generated an audit archive for the previous audit record. Example 3.27 shows the ISSO querying the archive record johns\_test. Now that the admin has verified that the audit archive is complete, the admin deletes the audit record, as shown in Example 3.28. DELETEAUDIT records apply to the preceding GETAUDITRPT records. For example:

```
GETAUDITRPT @ 20001005100007 : Audit Report Generated for
User gen_user From Date 20001005085925 To Date
20001005095925 For Event QUERY from Daleth Gatekeeper
```

```
GETAUDITRPT @ 20001005100507 : Audit Report Generated for
User gen_user From Date 20001005095925 To Date
20001005095925 For Event LOGIN from Daleth Gatekeeper
```

```
DELETEAUDIT @ 20001013113608: Audit Deleted for User
gen_user from Daleth Gatekeeper
```

**Example 3.29 - Delete an Audit Record**

In this example, the ISSO deleted all LOGIN records for the user gen\_user. The QUERY records are still in the database.

**3.3.2 Audited Information**

*Check the boxes corresponding to the information provided for the audited events.*

<input checked="" type="checkbox"/>	Userid	<input checked="" type="checkbox"/>	Type of Event or Action	<input type="checkbox"/>	Resources
<input checked="" type="checkbox"/>	Time	<input checked="" type="checkbox"/>	Terminal or Workstation ID	<input type="checkbox"/>	System location
<input checked="" type="checkbox"/>	Date	<input checked="" type="checkbox"/>	Success or failure of the event	<input type="checkbox"/>	Entity that initiated transaction

**Table 3.6 – Audited Information**

**3.3.3 Audited Activities**

*Check the box corresponding to the types of activities audited. Windows NT specific audit activities can be selected in a specific box below.*

EVENT DESCRIPTION	DO YOU AUDIT SUCCESS	Do you audit FAILURE	EVENT DESCRIPTION	SUCCESS	FAILURE
Logins	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Logoffs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Printing	<input type="checkbox"/>	<input type="checkbox"/>	Copying data to removable media	<input type="checkbox"/>	<input type="checkbox"/>
Use of Superuser or root privileges	<input type="checkbox"/>	<input type="checkbox"/>	Read a file or directory	<input type="checkbox"/>	<input type="checkbox"/>
Creation of a file or data element(s)	<input type="checkbox"/>	<input type="checkbox"/>	Deletion of a file or data element(s)	<input type="checkbox"/>	<input type="checkbox"/>
Attempts to change data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Use of applications	<input type="checkbox"/>	<input type="checkbox"/>
Security relevant objects and incidents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Console	<input type="checkbox"/>	<input type="checkbox"/>

**Table 3.7a – Audit Event Descriptions**

<input checked="" type="checkbox"/>	The audit log is archived on magnetic media and maintained for a time period.			
	Enter the time period for on-line storage: SITE POLICY			
	<input type="checkbox"/> days	<input type="checkbox"/> weeks	<input type="checkbox"/> months	<input type="checkbox"/> years

**Table 3.7b – Audit Archiving**

**3.3.4 Audit Review**

*Identify the individual responsible for ensuring the review of audit trails and how often the reviews are performed.*

FINAL

SITE POLICY

### **3.3.5 Audit Handling**

*Describe the procedures for handling discrepancies found during audit trail reviews.*

SITE POLICY

## **3.4 Marking and Labeling**

### **3.4.1 Hardware**

*Describe how the system hardware will be labeled to identify its classification level, compartments, and handling controls.*

SITE POLICY

### **3.4.2 Storage Media**

*Describe how the data storage media will be labeled to identify the classification level, compartments, handling controls, and information contents.*

SITE POLICY

### **3.4.3 Hardcopy Output**

*Discuss procedures for marking and controlling system printouts.*

SITE POLICY

## **3.5 Sanitization and Destruction**

### **3.5.1 Hardware**

*Describe the procedures and methods used to sanitize hardware (volatile or nonvolatile components). If applicable, describe the procedures for declassification.*

SITE POLICY

### **3.5.2 Software**

*Describe the procedures or methods used to clear, sanitize, and destroy the data storage media. If applicable, describe the procedures for declassification.*

SITE POLICY

## **3.6 Software Security Procedures**

UNCLASSIFIED

FINAL

### **3.6.1 Procurement**

*Describe the procedures for procuring and introducing system software.*

SITE POLICY

### **3.6.2 Impact Evaluation**

*Describe the procedures for evaluating system software for security impacts.*

SITE POLICY

### **3.6.3 Virus and Malicious Code Protection**

*Describe procedures for protecting software from computer viruses and malicious code and for reporting and responding to incidents.*

SITE POLICY

### **3.6.4 Maintenance**

*Indicate whether a separate version of the operating system software will be used for maintenance.*

SITE POLICY

## **3.7 Media Movement**

### **3.7.1 Into and Out of Secure Facility**

*Describe the procedures or receipting methods for moving data storage media into and out of the secure facility.*

SITE POLICY

### **3.7.2 Copy/Review/Release**

*Describe the procedures for copying, reviewing, and releasing information on data storage media.*

SITE POLICY

## **3.8 Hardware control**

### **3.8.1 System Transport**

*Describe the procedures or receipting methods used to release and transport the system hardware from the secure facility.*

SITE POLICY

UNCLASSIFIED

### **3.8.2 System Relocation**

*Describe the procedures or receipting methods for temporarily or permanently relocating the system hardware within the secure facility.*

SITE POLICY

### **3.8.3 Control/Operation/Maintenance**

*Describe the procedures for the secure control, operation, and maintenance of the hardware. If they have been authorized, describe the procedures for using readily transportable systems (i.e. laptops) for unclassified processing in the secure facility.*

SITE POLICY

### **3.8.4 Hardware Acquisition**

*Describe the procedures for introducing hardware into the secure facility.*

SITE POLICY

## **3.9 Web Protocol and Distributed/Collaborative Computing**

### **3.9.1 Web Server Security**

*For Web protocol systems, describe the security of the servers.*

Insecure operating services and programs, such as tftp, rlogin, rshell, etc. are disabled on Broadsword servers. Web server directory permissions are restricted to mitigate any risks of malicious code insertion at the server level.

### **3.9.2 Mobile Code**

*For Web protocol systems, describe the use of mobile code.*

The Broadsword client is a web-based interface into the Gatekeeper. This client makes use of HTML and Javascript to present information to the user. Javascript is used to implement context-sensitive buttons, cascading menus, and a map search utility. Javascript is classified as Type 3 mobile code in the DoD and IC community mobile code policies.

Additionally, the Broadsword client includes a signed Java applet, which is used for a graphical map interface. This is classified Type 2 mobile code in the DoD and IC community mobile code policies.

### **3.9.3 Executable Code**

*For Web protocol systems, describe how executable code is handled.*

N/A

**3.9.4 Collaborative Computing**

*If applicable, describe any collaborative computing process or applications.*

N/A

**3.9.5 Distributed Processing**

*If applicable, describe any distributed processing employed by the system.*

N/A

## 4 BACKUP POLICY AND PROCEDURES

*Describe the policy for backing up the system's information. This policy should reflect the system's designated Levels-of-Concern for Integrity and Availability. Provide detailed procedures for performing system backups.*

The following section will describe the procedure to store Broadwords Archived Files to tape. All other backup policy and procedures would be conducted according to the site policy.

### 4.1 Storing archived audit log records using offline tape storage

Begin by obtaining a shell prompt window with sufficient rights to read and delete the files under "/opt/bswd<version\_number>/audits", and also rights to read and write to the tape drive. This window can be obtained remotely by using telnet or rlogin, if either are configured as available, or by accessing the Broadsword system console directly. To obtain this window remotely, simply telnet or rlogin to the Broadsword server and login with a known username and password. Otherwise, if you are on the system console, login with a known username and password and obtain a shell window by using the popup menu on the desktop. Then, use the su command to make your effective userid "root":

Change effective userid to "root"

```
% su - root
```

#### Example 4.1 – Changing effective userid

The root account should have access to both the "/opt/bswd<version\_number>/audits" and the tape drive.

#### 4.1.1 Storing Audit Logs

Once you have successfully archived the desired audits records and removed them from the Broadsword Sybase Database as described above, insert the tape you wish to store audits on in the tape drive and execute the following:

Change your current directory to the audit archive directory and list the files

```
# cd /opt/bswd3.1/audits
# ls -l
```

#### Example 4.2 – Changing current directory

You should see at least the file you specified above when you archived the audit records desired

Check the status of the tape drive

## FINAL

```
# mt -f /dev/rmt/0 status
```

**Example 4.3 – Tape Drive Status**

Status should show the type of tape drive, not that the drive is offline. If your desired tape drive is known by a different filename, use that filename, i.e. /dev/rmt/1

Be sure the tape is rewound

```
# mt -f /dev/rmt/0 rewind
```

**Example 4.4 – Rewinding Tape**

Prompt should return after a short time

Archive the desired audits to tape

```
# tar cvf /dev/rmt/0 /opt/bswd3.1/audits/<filename>
```

**Example 4.5 – Archiving audits to tape**

Where <filename> is the name of the file you archived from within the Broadsword interface. You should see the name of the file on the screen as the archive is written to tape.

Remove the archived audit file from the hard disk

```
# rm /opt/bswd3.1/audits/<filename>
```

**Example 4.6 – Removing archived audits from file system**

Prompt should return after a short time

Eject the tape

```
# mt -f /dev/rmt/0 offline
```

**Example 4.7 – Ejecting tape**

The tape should eject from the tape drive.

Mark the tape properly, noting the filename contained on the tape, and store appropriately.

FINAL

## 5 RESTORATION POLICY AND PROCEDURES

*Describe the policy for restoring information to the system. This policy should reflect the system's designated Level-of-Concern for Availability. Provide detailed procedures for restoring information to the system, to include a full system recovery.*

### 5.1 Retrieving archived audit log records using offline tape storage

#### 5.1.1 Retrieving Broadsword audit logs

Begin by obtaining a shell prompt window with sufficient rights to read and delete the files under "/opt/bswd<version\_number>/audits", and also rights to read and write to the tape drive. This window can be obtained remotely by using telnet or rlogin, if either are configured as available, or by accessing the Broadsword system console directly. To obtain this window remotely, simply telnet or rlogin to the Broadsword server and login with a known username and password. Otherwise, if you are on the system console, login with a known username and password and obtain a shell window by using the popup menu on the desktop. Then, use the su command to make your effective userid "root":

Change effective userid to "root"

```
% su - root
```

#### Example 5.1 – Changing effective userid

The root account should have access to both the "/opt/bswd<version\_number>/audits" and the tape drive.

Insert the tape that contains the desired audits in the tape drive and execute the following:

Verify you will not overwrite an existing audit file

```
# cd /opt/bswd3.1/audits
# ls -l
```

#### Example 5.2 – Changing directory

Simply be sure there is not already a file that exists with the same filename as the one you intend to retrieve

Check the status of the tape drive

```
# mt -f /dev/rmt/0 status
```

#### Example 5.3 – Check Tape Drive Status

Status should show the type of tape drive, not that the drive is offline. If your desired tape drive is known by a different filename, use that filename, i.e. /dev/rmt/1

UNCLASSIFIED

FINAL

Be sure the tape is rewound

```
# mt -f /dev/rmt/0 rewind
(Prompt should return after a short time)
```

Extract the audits from tape

```
# tar xvf /dev/rmt/0
```

**Example 5.4 – Extract Audits**

The archived audit filename will appear on the screen and when the process is complete, the file will appear in the /opt/bswd<version\_number>/audits directory

Eject the tape

```
# mt -f /dev/rmt/0 offline
```

**Example 5.5 – Eject Tape**

Tape should eject from the tape drive.

You should now be able to query the restored archived audit records with the ISSO --> Archived Audit Logs screen.

All other restoration policy and procedures would be conducted according to the site policy.

FINAL

## **6 KNOWN VULNERABILITIES AND RISK MITIGATION APPROACH**

*Describe known security vulnerabilities regarding the configuration and use of administrative functions.*

Broadsword is not currently running under Trusted Solaris. If a user is able to gain access as the root user, it would be possible to circumvent several of the security mechanisms

*Identify any risk mitigation approaches to alleviate identified vulnerabilities.*

Broadsword is investigating the migration to Trusted Solaris