

Trusted Facility Manual (TFM) for the Trusted Transfer Agent (TTA)

Version 1.0.2

February 2002

Prepared for:

AFRL/IFEB

32 Brooks Road

Rome, New York

Prepared By:

Dolphin Technology, Inc.

1300B Floyd Ave

Rome, New York 13440

1	Introduction.....	4
1.1	Introduction to the TTA TFM.....	4
1.1.1	Purpose of the manual.....	4
1.1.2	Recommended use of the manual.....	4
1.2	Audience	4
1.3	Scope.....	4

DRAFT

1.4	Product Trademark Registration.....	4
1.5	References.....	5
2	System Security Overview.....	6
2.1	System Environment.....	6
2.2	System and Security Management Roles and Responsibilities	8
2.3	System User Access Policy.....	10
2.3.1	User Access Controls	10
2.3.2	Assignment and Control of Authenticators.....	10
2.3.3	IS User Access	11
2.3.4	Privileged User Access	11
2.3.5	Password Changes, Password Generation	11
2.3.6	Number of Allowed Login Attempts	11
2.3.7	Account Lockout.....	12
2.4	User Groups and Access Rights.....	12
2.4.1	User Groups	12
2.4.2	System Files	13
2.4.3	System Access Rights	13
2.4.4	Audit Log Access.....	13
2.4.5	Privileged Users	14
2.4.6	DAC/MAC	14
3	Security Related Features And Procedures.....	15
3.1	Broadsword Gatekeeper and ISSE Guard Dependencies	15
3.2	Security Modifications to Solaris.....	16
3.3	Non-releasable Field Substitution.....	18
3.4	MD5 Integrity sealing	18
3.5	Protection of the Security Support Structure.	19
3.6	Security Features and Assurances.....	19
3.6.1	Incident Reporting.....	19
3.6.2	Automatic shutdown.....	20

DRAFT

3.6.3	Disabled Remote Access.....	20
3.6.4	Change Control.....	20
3.6.5	Configuration Management	20
3.6.6	Security Filtering.....	21
3.6.7	System Startup	26
3.6.8	System Shutdown.....	28
3.7	Auditing	29
3.7.1	Levels of Auditing	29
3.7.2	Audited Information.....	30
3.7.3	Audited Activities	30
3.7.4	TTA Audit System Failure.....	32
3.7.5	TTA Audit Reduction.....	32
3.7.6	TTA Audit Archival and Restoration.....	34
3.8	Marking and Labeling.....	37
3.8.1	Hardware, Storage Media, and Hardcopy Output.....	37
3.9	Software Security Procedures	37
3.9.1	Procurement	37
3.9.2	Protection from Viruses and Malicious Code.....	37
3.9.3	Maintenance	37
3.10	Media Movement	37
3.11	Hardware control.....	38
3.12	Web Protocol and Distributed/Collaborative Computing.....	38
4	Backup Policy And Procedures	39
5	Restoration Policy And Procedures	40
6	Known Vulnerabilities And Risk Mitigation Approach.....	41
Appendix A	Exclusive Global Filter Expressions	42

1 INTRODUCTION

1.1 Introduction to the TTA TFM

1.1.1 Purpose of the manual

This manual is intended to act as a guide to help ensure the secure configuration and installation of the TTA version 1.0.2 system, to inform the security and system administrator personnel of the privileges and security mechanisms which TTA takes advantage of, and to provide a summary of the steps and commands required to securely operate and administer the TTA system.

1.1.2 Recommended use of the manual

This manual should be used to review the skills and systems background necessary for security and system administrator personnel tasked with operating the TTA system. Additionally, security and system administrator personnel should review and understand chapters 5, 6, and 7 of the *System Installation and Maintenance Guide for Broadword v 3.1* describing TTA configuration and installation, and *Broadsword Gatekeeper System Security Authorization Agreement* describing various system security aspects of the Broadsword Gatekeeper system.

1.2 Audience

This document is intended only for privileged users such as system administrators, ISSOs and ISSMs.

1.3 Scope

The scope of this guide addresses the TTA privileged user's responsibilities to include all actions necessary to operate and maintain TTA on a day-to-day basis, and to ensure that the necessary security related protections are installed, configured, and operating properly. Steps to be performed by the TTA administrator include starting, stopping, status monitoring, audit archival, and audit analysis. The TTA administrator working in coordination with the site ISSO or ISSM should perform steps that modify the security policy enforced by TTA involving the configuration of the Exclusive Global Filters and Inclusive Field Level Filters.

1.4 Product Trademark Registration

The TTA system resides on two Sun workstations running the Solaris® Operating System software, and specific components of TTA are developed using Java® technology. Sun, Sun Microsystems, Solaris and Java are registered trademarks of Sun Microsystems, Inc.. The Broadsword Gatekeeper, a component of the TTA system uses the Sybase® Database Management System. Sybase is a registered trademark of Sybase, Inc..

1.5 References

- System Installation and Maintenance Guide for Broadsword v3.1*, AFRL/IFEB, 2002.
- Broadsword Gatekeeper System Security Authorization Agreement (SSAA)*, 2002.
- Broadsword Gatekeeper Trusted Facility Manual*, 2002.
- Defense Intelligence Agency C2 Security Configuration and C2 Setup Checklist*, DRAFT, For Solaris 2.5.1 through Solaris 2.8 Systems, DIA, 2001.
- Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems*, March 31, 2001.
- DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide*, April 2000, DS-2610-142-01.
- Information Support Server Environment (ISSE) Guard System v3.2 Installation Guide for Trusted Solaris 2.5.1*, July 1999, Control No. P42-3.1-GIG-0799-A0.
- Information Support Server Environment (ISSE) Guard System v3.2 System Security Authorization Agreement (SSAA)*, Dolphin Technology, 2001.
- Information Support Server Environment (ISSE) Guard v3.2 Administrative Standard Operating Procedures*, Dolphin Technology, 2001.
- Information Support Server Environment (ISSE) Guard v3.2 Installation Guide for Trusted Solaris 2.5.1*, Dolphin Technology, 2001.
- Information Support Server Environment (ISSE) Guard v3.2 Trusted Facility User's Guide (TFUG)*, Dolphin Technology, 2001.
- Solaris 2.5[.1] Security Checklist*, Report # C4-030R-98, National Security Agency, 24 September 1998.

2 SYSTEM SECURITY OVERVIEW

2.1 System Environment

Organizations use Broadsword Gatekeepers to access information including imagery, messages, and database products resident on backside source systems. In support of this objective, personnel must frequently access and retrieve information from various data sources and analyze and combine this information to generate new products.

TTA, working in combination with Broadsword's Gatekeeper and the Information Support Server Environment (ISSE) Guard, provide a computer system capable of facilitating access to information across security boundaries. The integrated TTA-Gatekeeper-ISSE Guard architecture, depicted in Figure 2.1-1 is capable of supporting a variety of user needs and site objectives. The architecture consists of a high side and low side Broadsword Gatekeeper community of interest (COI) including numerous Gatekeepers, back side sources, and a Keymaster all integrated via JWICS on the high side and SIPRNET on the low side. Interfacing the high side and low side Gatekeeper COIs is accomplished via a bridge comprised of 3 systems, the TTA high side system, ISSE Guard, and a TTA low side system. The DIA has designated that the TTA high and low systems be installed on dedicated platforms and meet the DCID 6/3 requirements for Protection Level 2 (PL2), and that the ISSE Guard be operated on a dedicated platform and meet the requirements for PL4.

DRAFT

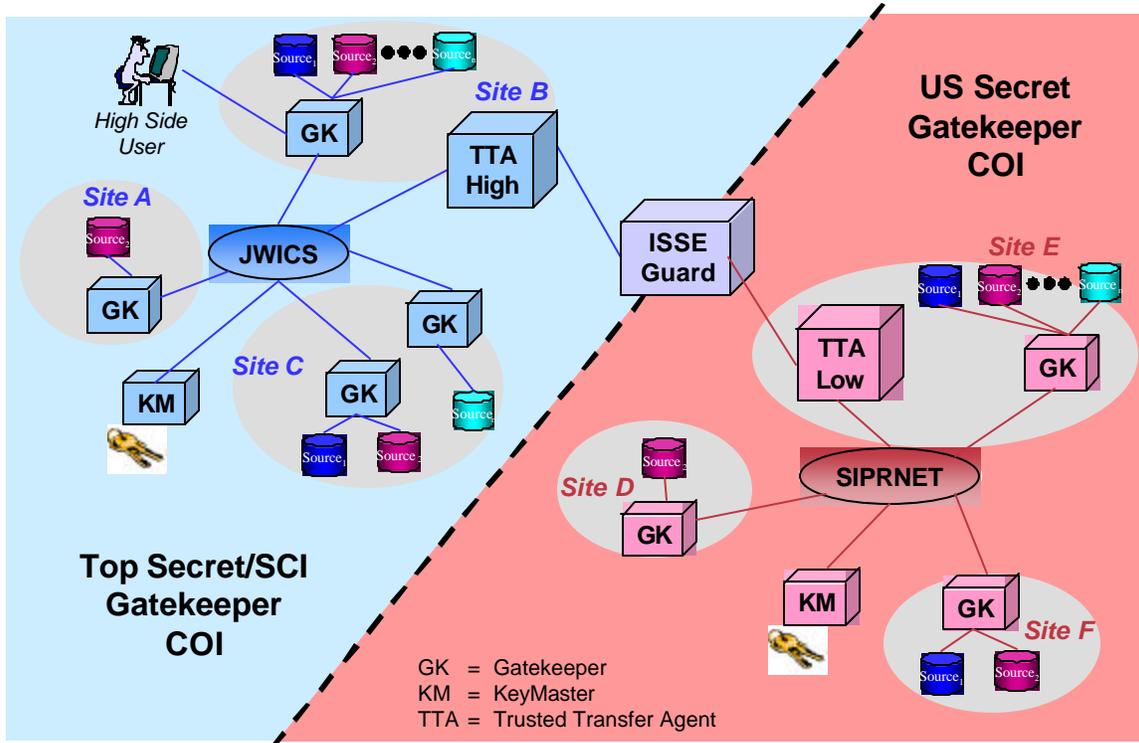


Figure 2.1-1: TTA Conceptual Architecture

With the Broadsword-TTA-ISSE Guard architecture personnel within the Gatekeeper Community of Interest (COI) operating at the Top Secret/SCI security level are able to access data produced and maintained in the Gatekeeper COI operating at the US Secret security level. Because the TS/SCI security level dominates, the TS/SCI domain is referred to as the “high side” and the US Secret domain is referred to as the “low side”. Analysts tasked with producing products for release to the Secret level user may use the system to initially confirm that the desired product does or does not already exist in the warfighter environment. Subsequently, the analyst may use the system to acquire information to construct composite products (which requires that a variety of source information be integrated) necessitating that various systems and data types (some at the low side security level) be accessed, and used.

Operational military organizations are continually being asked to generate better, more accurate results faster with less people, less support funding, and within less physical space. The use of TTA allows organizations to expedite the inter-domain information transfer process. Furthermore, the employment of TTA allows them to accomplish this with less administrative burden in terms of personnel, hours spent, and overall equipment cost. This savings is achieved by reducing the need for duplicate back-side source systems existing at different security levels, and eliminating the need for duplicate user terminals to access different security domains.

TTA works in concert with the ISSE guard to provide an automated security bridge across which information is allowed to flow between security domains. This increased

DRAFT

functionality does not come without risk. The following security vulnerabilities are identified and addressed by TTA security features:

- Disclosure of information at an incorrect security level (namely, disclosure of TS/SCI information to the Secret domain) initiated via inadvertent or malicious high side activities or as a result of improper configuration.
- Disclosure of information at an incorrect security level initiated via a malicious low side penetration.
- Denial of service attacks degrading performance or rendering the TTA interface inoperable, thus denying valid high side users the ability to query and retrieve products from the low side domain.
- Spoofing attacks in which TTA provides information to operational users that has been tampered with and may contain misinformation.
- Passage of information across the TTA interface containing viruses.

The remainder of this document describes the many security related features that have been included in the TTA to mitigate the risks associated with these vulnerabilities.

2.2 System and Security Management Roles and Responsibilities

The following describes the roles and responsibilities of individuals with respect to the secure operation of the TTA

Information System Security Manager (ISSM): The Site ISSM, responsible for an organization's IS security program, is responsible for the following TTA specific activities:

- Maintaining the repository for TTA system certification documentation and modifications.
- Actively participating in the TTA configuration management process, identifying proposed changes that may impact the TTA system or site security posture.
- Ensuring that TTA is developed, procured, or operated by the Site in a manner that meets and maintains applicable security requirements.
- Acting as focal point for TTA certification and accreditation actions possibly including acting as Test Director during security testing.
- Implementing and enforcing IS security policies as they apply to the TTA system.
- Reviewing the Broadsword/TTA SSAA to ensure that site policies and procedures are reflected as appropriate and endorsing those found to be acceptable.
- Overseeing all ISSOs to ensure they are following established information security policies and procedures.

DRAFT

- Developing procedures for responding to security incidents, and for investigating and reporting security violations and incidents related to the TTA system.
- Ensuring proper protection or corrective measures have been taken when an incident or vulnerability has been discovered within the TTA system.
- Ensuring that data ownership and responsibilities are established for the TTA system, including accountability, access rights, and special handling requirements.

Information System Security Officer (ISSO): The ISSO is responsible for ensuring that operational security is maintained for an IS. TTA system specific responsibilities include:

- Ensuring the TTA system is operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the SSAA.
- Ensuring that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access to the TTA.
- Reporting all security-related incidents to the ISSM.
- Initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered relevant to the TTA system.
- Conducting periodic reviews of the TTA system to ensure compliance with the Broadsword/TTA SSAA.
- Ensuring configuration management (CM) for security-relevant TTA software, hardware, and firmware is maintained and documented.
- Ensuring that TTA system recovery processes are monitored to ensure that security features and procedures are properly restored.
- Ensuring all TTA relevant security-related documentation is current and accessible to properly authorized individuals.
- Formally notifying the ISSM (or SCO/DCO, as appropriate) when changes occur to the TTA system that might affect accreditation.
- Ensuring that system security requirements are addressed during all phases of the TTA system life cycle.
- Following procedures developed by the ISSM for authorizing TTA related software and hardware use before implementation on the system.

TTA System Administrator: The TTA System Administrator is a UNIX system administrator role responsible for the day-to-day operation and maintenance of the TTA systems. The TTA system consists of a high side platform operating in the TS/SCI domain and a low side system operating in the US Secret domain. The system administrator role may consist of maintaining one of both of the TTA platforms

DRAFT

depending on the degree of geographic separation between them. Specific responsibilities include:

- Starting, stopping and restarting the TTA applications.
- Process monitoring of the TTA applications to determine their status.
- Audit log examination and/or reduction to identify and investigate security-related and non-security-related events.
- Audit log archival to tape, audit log tape maintenance, and audit log tape recovery.
- Periodic examination of Exclusive Global Word and Inclusive Field Level Filtering Criteria.
- Modification of Exclusive Global Word and Inclusive Field Level Filter Criteria (to be performed in coordination with the ISSO/ISSM)
- Supporting/oversight of all phases of the TTA life cycle including installation, configuration, and testing of all TTA versions, patches, and upgrades.
- Coordination of TTA operation with other Broadword Gatekeeper and ISSE Guard system administrators.
- Reporting all security-related incidents to the ISSO/ISSM.

Computer Operators/Non-Privileged Users: N/A, TTA is system-to-system interface and thus does not directly interface to any computer operators or non-privileged users.

2.3 System User Access Policy

2.3.1 User Access Controls

All user access to the TTA High and Low systems is controlled via standard Unix login and password capabilities provided as part of the Solaris 2.6 Operating system. Since TTA is a dedicated component of a security interface only privileged users are provided login access to the systems. Privileged users gain privileges by their membership in groups as defined in section 2.4.1 and access to the root account as described in section 2.4.3. After logging into the TTA high or low workstation, discretionary access controls (DAC) based on the Unix group ID(s) assigned to the login account are used to control access to the various files/processes of TTA. Additionally, the TCP Wrappers application has been installed on the TTA platforms and has been configured to deny remote access to such TCP/IP services as telnet, rsh, rlogin, etc.

2.3.2 Assignment and Control of Authenticators

All TTA login accounts and assignment of cgiAdmin or cgiuser privileges need to be reviewed and approved by the ISSM. Once approved, the system administrator can setup the required login accounts on the TTA workstation.

DRAFT

2.3.3 IS User Access

Check all boxes that apply to the passwords assigned to the IS users.

- All users have their own unique userid and unique password.
- Some users share a userid and password. (Explain below)
- Some users share a password. (Explain below)

2.3.4 Privileged User Access

Select only one level of access.

The privileged users have a unique userid and unique password at the:

- user level of access.
- superuser level of access.

Explanation: In accordance with the NSA recommendations for secure configuration of Solaris non-login superuser (root) account exists on the TTA High and Low platforms. System administrators requiring root access are provided the appropriate password and must first login using unique userid and password. Once logged in, they can then execute a switch user command to gain root access using the root password. Since both the initial login, and the switch user command are audited events, that actions performed as root can be traced back to a unique individual via audit log examination.

2.3.5 Password Changes, Password Generation

Select one box only.

- Passwords are NOT changed.
- 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.
- Users are forced to change their passwords every . . . *(Check all that apply)*
 - Month 6 months Year NEVER After Initial Login
 - Other (90 days): Password updates are made in accordance with N-SP password change policy.

Explanation: In accordance with DIA recommendations, user accounts on the TTA High and Low platforms must include a password. Passwords are configured to be 8 characters in length, expiring every 90 days with a 5 day expiration warning.

2.3.6 Number of Allowed Login Attempts

Select one box only.

If a user enters the wrong userid or password:

- A time-out interval is enforced.
- NOTHING happens. The user can try to logon as many times as he or she wishes.

DRAFT

<input checked="" type="checkbox"/> Maximum number of attempts: 3

2.3.7 Account Lockout

Select all that apply.

If a user's account is locked out due to excessive invalid logon attempts, who is authorized to reinstate the user's account?

- System Administrator
- ISSO
- Superuser
- Account Owner
- System automatically reinstates the account after a specified time period
- Other:(Specify)

2.4 User Groups and Access Rights

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 administrator.
<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 checked="" type="checkbox"/>	Users are assigned to different groups depending on need-to-know and work assignments.
<input checked="" type="checkbox"/>	User groups have different privileges/access rights depending on need-to-know and work assignments.
<input type="checkbox"/>	Other: Specify

Explanation: It is recommended that all TTA system administrator individuals be placed in the primary group of *tta*, with membership in the secondary groups of *cgiadmin*, *cgiuser*, *bswd*. These memberships allow the TTA administrator to access and control the full breadth of TTA system functionality. Specific data files, scripts, executables, and libraries essential to the secure operation of TTA are protected by assigning file access privileges making them accessible to only members of the group. Specifically, membership in these groups provides the following:

DRAFT

- **tta**: Allows an administrator to start, stop, monitor and administer all TTA specific processes including execution of the Field Level Filter Administration Tool.
- **cgadmin**: Allows an administrator to access the CGI Administrator application through which the parameters describing how TTA communicates with the ISSE Guard are defined.
- **cguser**: Allows an administrator to access the Common Guard Interface capabilities which are able to communicate with the ISSE Guard.
- **bswd**: Allows an administrator to access and debug Broadsword Gatekeeper related functionality running on the TTA platform.

2.4.2 System Files

Select *ONE* box, only.

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

Explanation: System files can only be changed by someone using the **root** username. Since the **root** account on TTA systems is configured as a non-login account, privileged users such as TTA administrators, ISSOs, and ISMs need to log into the system using their individual usernames and passwords, then execute the Unix switch user command (**su**) to **root** to gain **root** privileges and change the configuration and/or content of system files.

2.4.3 System Access Rights

Select *ONE* box, only.

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

Explanation: Only individuals with root access can set the system access rights for other users.

2.4.4 Audit Log Access

Select *all* boxes that apply.

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

DRAFT

Explanation: The TTA audit log maintained under Solaris in */var/log/syslog* is owned by the user *root* who has read and modify ability on the log. All other users possessing logins to the TTA systems have read-only access to the log.

2.4.5 Privileged Users

As discussed previously, privileged users gain privileges by their membership in groups as defined in section 2.4.1 and the root account as described in section 2.4.3. TTA is not accessed by non-privileged users. Thus all users of the system who possess used IDs on the system are TTA administrators, ISSOs, or ISSMs. It is assumed that these users are fluent in Solaris system operation and administration, TTA operation and administration, and site defined security policies and procedures. Though there are no TTA imposed limits on the number of privileged users that can be defined for the TTA system, from a practical sense the number of privileged users allowed access to the TTA should be minimized to approximately 10 or less so that system administration and security policy changes can be easily coordinated and communicated amongst all privileged users.

2.4.6 DAC/MAC

The TTA system implements Discretionary Access Control (DAC) over the system objects (executables, files, directories, etc.) using capabilities in Sun's Solaris operating system. Object access is controlled by comparing the subject's ID (user's ID, process ID, etc.) with object ownership and access permission information. These controls are *discretionary* in the sense that a user or process given discretionary access to information is capable of passing that information along to another subject. Mandatory Access Controls (MAC) are not available on the TTA workstations.

Both DAC and Mandatory Access Control (MAC) are implemented on the ISSE Guard using capabilities in Sun's Trusted Solaris Operating System. For a detailed description of the security features provided in the ISSE Guard, please refer to the *ISSE Guard v3.2 System Security Authorization Agreement*. MAC in the ISSE Guard is implemented via security labels associated with all subjects (users, processes, etc.) and objects (files, directories, etc.) specifying the security level (or range) at which it is allowed to operate. The MAC policy in the ISSE Guard compares the sensitivity level at which the user is working to the sensitivity label of the object being accessed and refuses access unless certain MAC checks are passed. The controls are *mandatory* because the labeling of information happens automatically, and ordinary users cannot change labels unless authorized by an administrator.

3 SECURITY RELATED FEATURES AND PROCEDURES

This section describes the various security features of the TTA systems and, where applicable, provides detailed instructions for operating specific security related aspects of the TTA system. Where applicable, it also describes the security operating procedures for the system with respect to users, roles, and responsibilities. Topics addressed in this section include:

- Broadsword gatekeeper and ISSE Guard dependencies
- Security modifications to Solaris
- Non-releasable field substitution
- MD5 integrity sealing
- Automatic shutdown
- Disabled remote access
- Security filtering
- Protection from viruses and malicious code
- System startup, shutdown, and status monitoring
- Audit record description, viewing, reduction archival, recovery and failover.
- Software, media, and hardware control procedures
- System security policy maintenance

Note: Unless otherwise stated, the steps in the following sections are performed from within the C Shell. System prompts are shown as either a “%” for TTA administrators and a “#” for root administrators

Note: Some of the steps described below refer to the directories in which the TTA applications have been installed. In the following steps *<full path to tta_v1.0.2_high>* will denote the high side installation directory, *<full path to tta_v1.0.2_low>* will denote the low side installation directory, and *<full path to tta_v1.0.2_high_or_low>* will denote either the low side or high side installation directory, whichever is applicable.

3.1 Broadsword Gatekeeper and ISSE Guard Dependencies

The TTA systems form an interface between the Broadsword Gatekeeper systems and the Information Support Server Environment (ISSE) Guard. To ensure proper, secure operation of this interface both the ISSE Guard and the Broadsword Gatekeepers need to be properly configured and maintained. ISSE Guard needs to be configured and administered in accordance with the *Information Support Server Environment (ISSE)*

DRAFT

Guard System v3.2 Installation Guide and the *Information Support Server Environment (ISSE) Guard System v3.2 Trusted Facility User's Guide (TFUG)*. The Broadsword Gatekeepers connecting to the TTA need to be configured and administered in accordance with the *Broadsword Gatekeeper System Security Authorization Agreement (SSAA)* and the *Trusted Facility Manual for the Broadsword Gatekeeper*.

3.2 Security Modifications to Solaris

The TTA system works in concert with the ISSE Guard to form a bridge capable of automatically moving information across security domains. It is imperative that the underlying operating system upon which TTA operates be configured to reduce and/or eliminate a variety of known security related system vulnerabilities. This section provides a general description of the necessary Solaris modifications, specific instructions for securely configuring Solaris in support of the TTA system are provided in Chapter 5 of the *System Installation and Maintenance Guide for Broadsword v3.1*. These recommendations are based on the recommendations provided by the Defense Intelligence Agency and documented in the *Defense Intelligence Agency C2 Security Configuration and C2 Setup Checklist*¹.

The following is a summary of the security-related Solaris modifications that need to be performed in support of the TTA system on both the high side and low side TTA platforms:

- Limit the use of the **su** command by creating the group **wheel** and changing ownership to **wheel**.
- Install the Basic Security Module (BSM).
- Remove the **uucp** and **nuucp** users and all files and directories owned by these user ids.
- Force the system to clean up files in **/var/tmp**.
- Remove unnecessary start up scripts in **/etc/rc2.d** and **/etc/rc3.d** including: **S76snmpdx**, **S72autoinstall**, **S30sysid.net**, **S80PRESERVE**, **S73nfs.client** and **S74autofs**.
- Modify the **/etc/init.d/inetinit** file to turn off IP forwarding.
- Modify the **/etc/default/inetinit** file to generate unique-per-connection-id sequence numbers.
- Enforce the "no" router policy.
- Turn off the multicast interface in **/etc/init.d/inetsvc**.
- Remove crontabs for **adm**, **sys**, **lp**, **uucp**.

¹ *Defense Intelligence Agency C2 Security Configuration and C2 Setup Checklist*, DRAFT, For Solaris 2.5.1 through Solaris 2.8 Systems, DIA, 2001.

DRAFT

- Change ownership and permissions on the following control directories to 0755 and owned by root: **/dev**, **/etc**, **/usr/bin**, **/usr/sbin**, **/usr/lib**, **/usr/ucb**, **/usr/dt**, **/usr/openwin**, **/usr/include**.
- Change all files with the ownership of **bin:bin** to **root:root**.
- Add the trace route option to **inetd** so that all incoming connections for the TCP services are logged.
- Add the **-t** option to the audit daemon to close the audit files.
- Disallow the **root** user from ftp'ing by creating the **/etc/ftpusers** file and placing the **root** user id in the file.
- Create a standard DOD access identification file to be printed as a login prompt.
- Reconfigure the **inetd.conf** file so that all unnecessary services are turned off.
- Remove and create **/dev/null** links to obsolete daemon processes including: **in.fingerd**, **in.named**, **in.rexecd**, **in.rlogind**, **in.routed**, **in.rshd**, **in.rwhod**, **in.talkd**, **in.telnetd**, **in.tftpd**, **in.tnamed**, **nscd**, **rpc.bootparamd**, **rpc.nisd**, **rpc.nispasswd**, **rpc.rexd**.
- Create **/dev/null** links for **-- /rhosts**, **/etc/hosts.equiv** and **/.netrc** to protect against trust relationships.
- Provide buffer overflow protection.
- Change ownership to **root:sys** and permissions to **644** on the **/etc/passwd** file.
- Change ownership to **root:sys** and permissions to **400** on the **/etc/shadow** file.
- Add additional logging to the system, routerlog, daemonlog, loginlog, and maillog.
- Reconfigure system auditing to log the following: **lo** (login / logout events), **ad** (administrative actions), **ex** (system calls), **fm** (file modifications), **na** (non-attribute events), **-fr** (unsuccessful file reads), **-fw** (unsuccessful file writes), **-fa** (unsuccessful access of file attributes), **-fc** (unsuccessful file creation), **-fd** (unsuccessful file deletion), **+ot** (everything else).
- Modify security of login sessions to enforce lock out on failed attempts.
- Install TCP Wrappers.
- Install a TCP Wrapped version of Sendmail.
- Install and Configure IP Filtering.
- Modify the **etc/password** file to ensure that all non-login accounts default to **bin/false** for their login shell.
- Set the maximum login attempts allowed to 3.
- Set the **password** on the **root** account.
- Modify **/etc/default/login** to not allow the **root** account to login from the console.
- Set the **eeprom security password**.

DRAFT

TTA Administrators, ISSOs and ISSMs should be familiar with these operating system modifications so that they can be aware of any possible subsequent modifications that may compromise the various protections afforded by the changes. The approval to operate TTA is contingent upon it running on this locked-down version of the Solaris operating system. These capabilities and services should not be changed by the TTA system administrator without prior coordination and approval of the Broadsword DODIIS Executive Agent (DExA): AC2ISRC/A2X, 240 Luke Ave, Bldg #1304, Bolling AFB, Washington DC 10332, Phone (202) 404-1278 or DSN 754-1278, and the Broadsword/TTA/ISSE Guard Program Management Office, AFRL/IFEB, 32 Brooks Road, Rome, New York, Phone (315) 330-3638 or DSN 587-3638.

3.3 Non-releasable Field Substitution

Included in the Broadsword gatekeeper product request messages originating on the high side are a number of sensitive fields that cannot be passed across the security boundary to the low side such as high side user IDs, passwords, and hostnames. To address this problem the TTA high side software automatically performs field substitution to sanitize the message. TTA replaces known sensitive fields with non-sensitive strings, and maintains a mapping table of the original and substituted field values. When the response arrives from the low side system via the ISSE Guard, an inverse table lookup is performed based on the fields in the message, and the substituted values in the message are replaced with the original values in the appropriate fields.

3.4 MD5 Integrity sealing

TTA working in concert with Broadsword Gatekeepers and the ISSE Guard provides an interface for information to flow from a high side client to a low side gatekeeper/source and back. It is important to ensure the integrity of the message and file contents is maintained from source to destination. To achieve this, a Message Digest 5 (MD5) integrity seal is assigned to all information immediately upon entering the TTA system. At many points during subsequent TTA processing, and within the ISSE Guard itself, this MD5 integrity seal is recalculated and compared to the original seal contained within the transaction to ensure that the data within the transaction has not been modified nor contaminated in any way.

Additionally, the integrity of information coming from the Broadsword client to the TTA high system containing user specified query statements is also ensured through the application and validation of an MD5 integrity seal. By validating this integrity seal upon receipt of the information, TTA ensures that the query statement, as generated by the Broadsword user, has arrived intact, and has not been modified or tampered with since it was authorized to be sent by the client.

All of the MD5 integrity sealing and verification occurring within the TTA occurs automatically. System administrators and ISSOs should be aware of its operations since specific audit log entries and automatic system shutdowns will occur if an MD5 error is encountered. Such MD5 errors may result from network communications errors, may signal that an incompatibility of software versions exists, or may indicate that someone is maliciously trying to mimic a valid Broadsword client or gatekeeper system.

DRAFT

3.5 Protection of the Security Support Structure.

TTA includes a variety of features to protect the security support structure. As discussed in other sections of this manual TTA utilizes:

- DAC with specific user and group privileges defined. (Sections 2.3 and 2.4)
- Operating system modifications to limit remote access to the system, restrict access via FTP to that essential for proper TTA operations, and enhance various security related aspects of the operating system such as auditing and password protection. (Section 3.2)
- Message field substitution to replace sensitive fields in the message prior to passing it across the security boundary. (Section 3.3)
- MD5 integrity sealing to ensure that message contents are not contaminated or tampered with during transit. (Section 3.4)
- Automatic shutdown when significant security related events are detected. (Section 3.6.2)
- Extensive security filtering defined via encrypted security filter configuration files. (Section 3.6.6)
- Script based startup, shutdown, and status monitoring to ensure proper execution of lengthy command sequences. (Sections 3.6.7 and 3.6.8)
- Extensive, multiple level event auditing to ensure end-to-end tracing of all communications through and significant actions within the TTA system. (Section 3.7)

3.6 Security Features and Assurances.

3.6.1 Incident Reporting

Upon installation at a site, the TTA systems will come under control of the site defined incident reporting process. If and when security related incidents are suspected the TTA system processes on both the high and low side TTA systems should be shutdown (if not already automatically shutdown) and their status verified in accordance with the instructions provided in section 3.6.8 of this guide. Next the system administrator working with the ISSO and/or ISSM should carefully examine the system audit trail (containing operating system events and detailed TTA system events) and the Broadsword audit log (containing Broadsword Gatekeeper events and high level TTA system events) to assess the cause and effect/damage of the suspected incident. If the incident is confirmed the site should then follow the site-defined incident reporting process which may include notification of the DAA and the Broadsword/TTA and ISSE Guard PMO.

DRAFT

3.6.2 Automatic shutdown

Specific types of events with potential security implications are continually monitored by TTA and if detected, the affected TTA system (high side or low side) is automatically shutdown. These events include detection of MD5 errors in messages flowing through the TTA, that the *syslog* daemon is not running, that security filter configuration files are not accessible, and that the ISSE Guard is not accessible. When these events occur and the TTA processes are shutdown, audit entries are written to the *syslog* describing the event (if the log daemon is running), and email describing the event is sent to all TTA administrators. TTA administrators and ISSOs should be aware of this feature since automatic shutdown, should it occur, may signal a serious security related event such as someone trying to maliciously penetrate through the TTA or that the ISSE Guard is not running or that proper system auditing is not occurring.

3.6.3 Disabled Remote Access

Remote access to the TTA is not allowed and is disabled at the time of installation by modifying/removing many of the standard Solaris system services file. FTP into the TTA system is allowed, but is restricted to specific hosts and userids necessary to allow the Broadsword Gatekeeper to communicate with the TTA systems via FTP through the proper application and configuration of TCP wrappers.

The TTA system administrators and ISSOs should be aware of this feature so that remote access is not inadvertently enabled and TTA integrity is compromised.

3.6.4 Change Control

No changes to the TTA system are to be made without prior coordination with the ISSO. These include changes to EGF or IFLF filters, changes to the Solaris configuration in the areas identified in section 3.2 of this manual, installation of operating system patches and or any modification/replacement of any TTA or Broadsword executables.

3.6.5 Configuration Management

Upon installation at a site, the TTA systems will come under control of the site defined configuration management process. Augmenting the site's capabilities is a rigorous configuration management and technology insertion process implemented under the direction of the Air Force Research Laboratory Information Handling Branch (AFRL/IFEB), and the PMO for the ISSE Guard System, Broadsword, and TTA. Requirements collection, Problem Report (PR) resolution, baseline tracking and version release are effected under the AFRL/IFEB Common User Baseline for the Intelligence Community (CUBIC) configuration management process. The CUBIC CM process dovetails with the development contractor CM process. These complimentary processes ensure the satisfaction of both functional and security requirements and that new versions and patches are released in a timely manner. These formal processes executed under the guidance of the Designated Accrediting Authorities (DAAs), result in the ability to field a system that is responsive to ever changing security threats and needs of the end user.

DRAFT

3.6.6 Security Filtering

Ultimately, the Broadsword user is responsible for reviewing the queries flowing from high to low and authorizing their release. To provide added protection and ensure that high side information is not inadvertently passed through the TTA and ISSE Guard to the low side, extensive security filtering operations are performed by the TTA Security Filtering Application (SFA) resident on the TTA high side platform. Since security policies change from time to time the security filters applied by the SFA are configurable by the ISSO working in concert with the TTA Administrator to enforce the appropriate security protection mechanisms.

TTA provides two types of filters:

1. The Exclusive Global Free-Text (EGF) filters leverage the Defense Intelligence Agency (DIA) accredited global message filter capability originally developed for the ISSE Guard application referred to as the “Dirty Word” filter. These filters consist of a list of words and/or phrases that are prohibited from appearing in any message flowing from high to low. They are referred to as exclusive filters because they specify values that are excluded from appearing in the message. The EGF filter configuration is stored within an encrypted text file. The filters are created/maintained by de-encrypting the text file, editing it using Unix text editors, and re-encrypting it. An initial EGF configuration file is provided with TTA when it is installed. This EFG file should be examined by the TTA administrators and ISSOs to understand the filtering criteria being applied, and tailored as needed to reflect site-specific filtering needs.
2. Inclusive Field Level (IFL) filters are derived from the queryable fields list and allowable values lists maintained within the Broadsword system. These filters identify specific fields and allowable values that must match those fields in a message in order for the message to pass the filter. These are inclusive filters because the field values in a message must be included in the allowable values list for that field. The IFL filter configuration is stored within an encrypted text file. The filters are created/maintained using the Field Level Filter Administration Tool (FLFAT). An initial IFLF configuration file is created upon activating the FLFAT tool for the first time which reflects the queryable inclusive fields currently configured in the Broadsword Gatekeeper. This initial configuration should be examined by the TTA administrators and ISSOs to understand the filtering criteria being applied, and tailored as needed to reflect site-specific filtering needs.

Figure 3.6-1 portrays the process flow for accomplishing filtering of messages flowing from high to low through the TTA. Upon arrival of a message destined for passage to the low side, a check is made to verify that EGF filters exist. If no filters exist, the message is not approved for High to Low transfer, the event is audited and the process is completed.

If EGF filters exist, the EGF filters are applied against the message, and any resulting filter errors are tabulated until all EGF filtering is complete. Upon successful completion of all EGF Filters, and, if the message is not a Broadsword Gatekeeper Client Query

DRAFT

Message (BGCQM), the message is then approved for passage to the low side system, the event is audited, and the process is completed.

If the message is a Broadsword Gatekeeper Client Query Message (BGCQM) and IFL filters are defined, IFL filters will be applied. If the BGCQM passes these filters, it is then approved for passage to the low side system, the event is audited, and the process is completed. If the message failed any of these filters the message is not approved for High to Low Transfer, the event is audited, and the process is completed for that message.

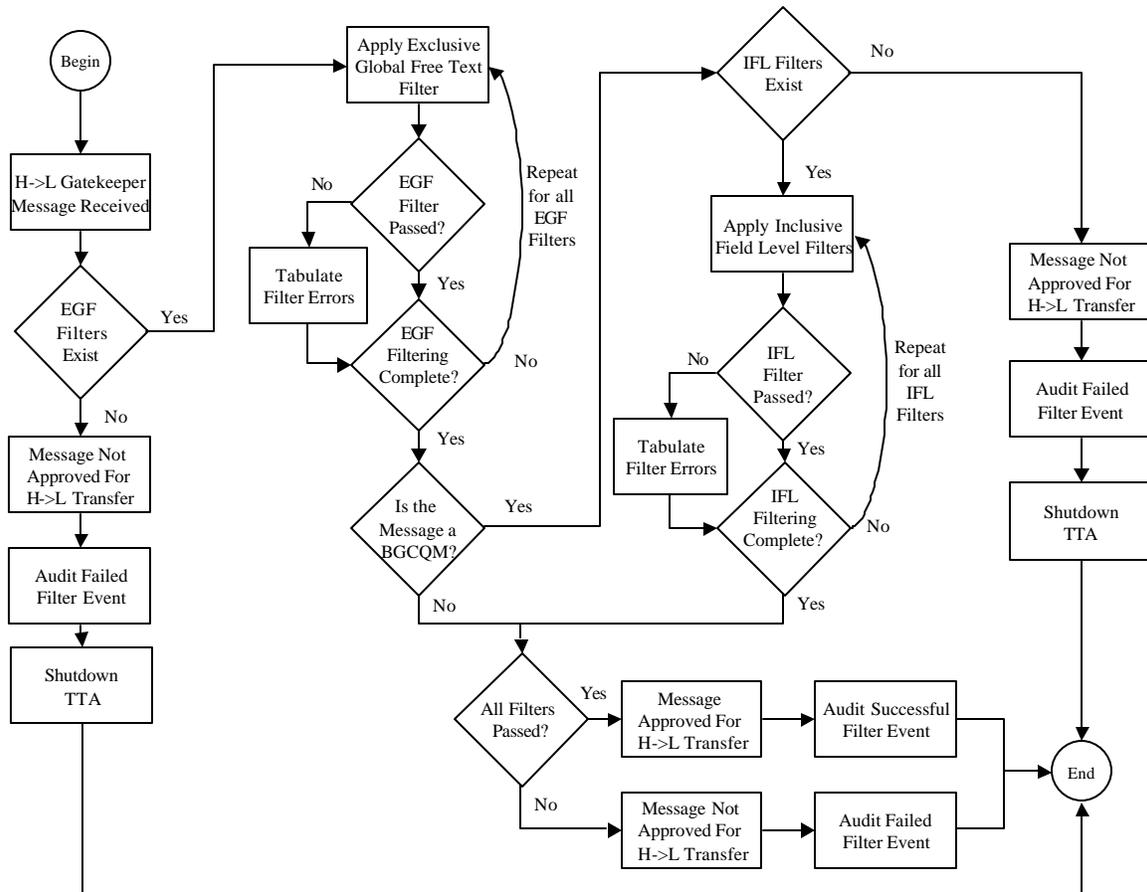


Figure 3.6-1: TTA Security Filtering Flow

The following sections describe EGF and IFL filters in more detail, along with the steps necessary to configure and administer these filters.

3.6.6.1 EGF Filter Configuration

The EGF filters use a global word list containing a list of words and/or phrases that are either not passable to the low side (e.g., classified code words, etc.) or strong indicators that the associated information in the message is not passable to the low side (e.g., security labels). By applying the EGF filters, it is determined if a message being passed through the TTA (and subsequently the ISSE Guard) from high to low contains any prohibited words. If a message is found to contain one or more words/phrases in the

DRAFT

prohibited word list the processing of the message is terminated, an error message describing the filter violation is generated and sent through established error reporting channels back to the originating user, and an error message is generated that is written to the system error log.

EGF filter configuration is controlled by an encrypted formatted text file, *dirty_word.cfg.ecr*. The EGF filter configuration file, located in the *<full path to tta_v1.0.2_high>/tta/config/<hostname>* directory, contains a list of regular expressions, simple words, or multi-word phrases to be searched for in the message data flowing from the High to the Low side TTA Gatekeepers. A regular expression may be added/deleted or modified by decrypting then editing the *dirty_word.cfg.ecr* file. Examples of regular expressions that can be included in the *dirty_word.cfg.ecr* file can be found in Appendix A.

Configuration of the EGF filters is stored in the *dirty_word.cfg.ecr* file. The following describes the steps required to modify this file on the High Side TTA Gatekeeper system.

1. Login to the system as a TTA Administrator.
2. Change the current working directory to the TTA home directory by executing the following command:

```
% cd < full path to tta_v1.0.2_high >/tta
```

3. Set up the appropriate runtime environment by executing the following command:

```
% source ./TTAvars.csh
```

4. Change the current working directory to the configured hostname directory where the TTA configuration files have been placed by executing the following command:

```
% cd < full path to tta_v1.0.2_high >/tta/config/<hostname>
```

5. Decrypt the configuration file found in the current directory by executing the following command.

```
% < full path to tta_v1.0.2_high >/tta/bin/<platform>/TtaEncrDecr  
./dirty_word.cfg d
```

6. The file can now be edited using any text editor.
7. After editing and saving the file, it must be encrypted. From the configured hostname directory, *< full path to tta_v1.0.2_high >/tta/config/<hostname>* execute the following command to encrypt the file.

```
% < full path to tta_v1.0.2_high >/tta/bin/<platform>/TtaEncrDecr  
./dirty_word.cfg e
```

DRAFT

3.6.6.2 IFLF Filter Configuration

IFL filters provide a finer granularity of security filter than the EGF filter described in Section 3.6.6.1. IFL filters are designed to check specific fields in the BGCQM to verify that the field value is a member of the set of permissible values allowed for that field.

IFL filter configuration is controlled by an encrypted formatted text file, *IFLF.cfg.ecr*. The text file consists of the Broadsword fields that have associated dropdown lists queryable through the TTA. Each field listed is followed by a set of permissible values for the field. The IFL filters are configurable by the ISSO to conform to changing security requirements and missions. The values used to configure the IFL filters are derived from queryable fields and allowable value lists maintained within the Broadsword system. Because of the close tie that must be maintained between Broadsword queryable fields/allowable values and the configuration of IFL filters, a tool exists to aid the ISSO in administering the IFL filters. This tool is referred to as the Field Level Filter Administration Tool (FLFAT). Figure 3.6-2 depicts the main window of the FLFAT.

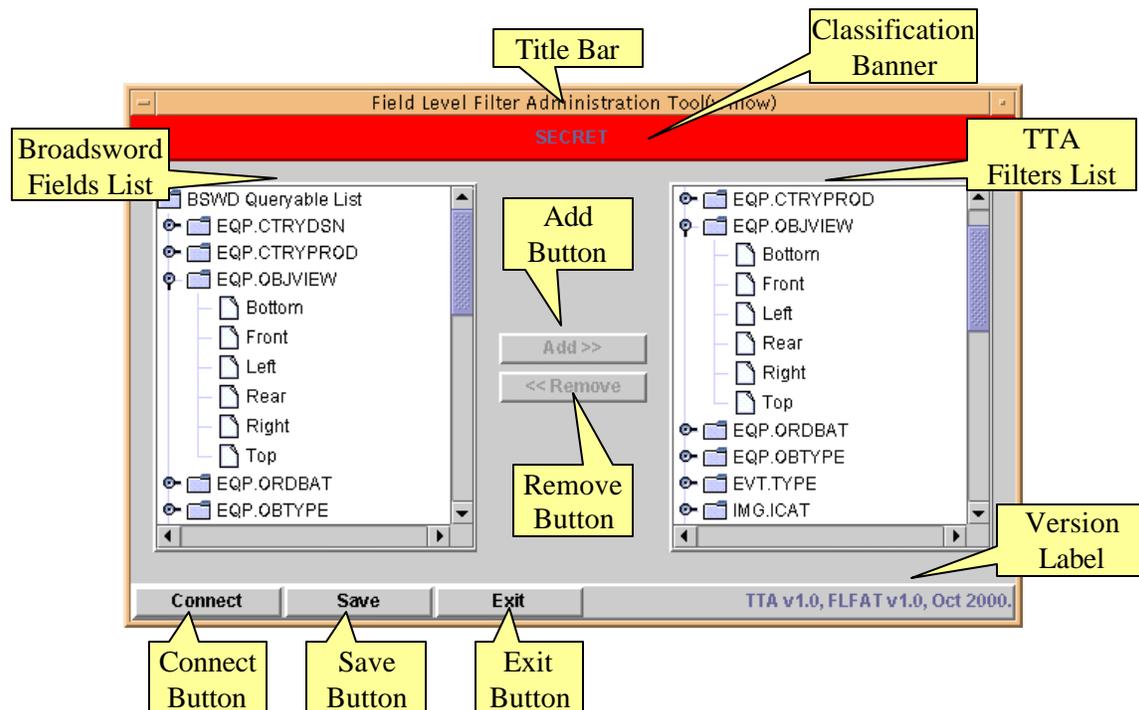


Figure 3.6-2: FLFAT Main Window

The window has the following major components:

- Title Bar displays the name of the application being executed with the hostname on which the software is running showed in parentheses.
- Classification Banner is a color-coded banner that displays the current classification level of the TTA system on which the tool is running.

DRAFT

- Broadsword Fields List contains the currently available list of Broadsword fields and their allowable values.
- TTA Filters List contains the current list of field level filters and the allowable values.
- Add Button adds the currently selected Broadsword field/allowable value (from the left hand scrolled area) to the TTA filters list (shown in the right hand scrolled area). Button is only enabled when a selection is made from the Broadsword Fields List.
- Remove Button removes the currently selected TTA filter field/allowable value (from the right hand scrolled area). Button is only enabled when a selection is made from the TTA Filters List.
- Connect Button establishes a connection to the TTA Gatekeeper and downloads the complete list of queryable fields and their associated data elements.
- Save Button extracts information from the current TTA Filters List (located in the right hand scrolled area), and creates and encrypts the *IFLF.cfg.ecr* file.
- Exit Button exits the FLFAT application. Prior to exiting, a check is made to determine if the TTA filter list has been modified and not saved. If so, the user is presented with the option to save the filters before the FLFAT application exits.
- Version Label is a static label identifying this specific version of the FLFAT, TTA, and the date of release.

The FLFAT application is a Java application that is executed by the ISSO on the TTA High Side Gatekeeper platform. The application is not accessible over the network and must be run on the platform for which the filters are intended. The application is located in the `<full path to tta_v1.0.2_high>/tta/scripts` directory and is named RUN_FLFAT. The FLFAT Application is started by issuing the command:

% RUN_FLFAT

Upon starting, the FLFAT will test to determine if a *IFLF.cfg.ecr* file exists on the system. If the file exists, it is read, de-encrypted, parsed, and the filter fields and allowable values contained in the file are used to initially populate the TTA Filter List.

Next, the FLFAT connects to the TTA High Gatekeeper and receives the connection response message containing the Broadsword queryable field list and allowable value lists. If the message is successfully received, the Broadsword Fields and allowable values are parsed from the message, and the Broadsword Fields list is populated. If the connection fails or the message isn't received, an error message is reported and audited.

If the *IFLF.cfg* file does not exist, the FLFAT application assumes it is in an initialization state and uses the entire default list provided by the TTA Gatekeeper. If this occurs, the user is presented with a warning message informing them that a default list is being used and they need to reconfigure the field level list to reflect the targeted classification level.

DRAFT

The ISSO then interacts with the FLFAT using the scrolled areas and button functionality provided in the Main Window. Filters are added by selecting a field and/or allowable value from the Broadsword Fields List (located in the left-hand scrolled area), and clicking the **Add** button. The selected field and/or allowable value will be added to the TTA Filters List (located in the right-hand scrolled area). Filters are removed by selecting a field and/or allowable value from the TTA Filters List, and clicking the **Remove** button. The selected field and/or allowable value will then be removed from the TTA Filters List. Following modification of the TTA Filters List, the filters are saved by clicking the **Save** Button. Doing so extracts information from the current TTA Filters List and updates/creates and re-encrypts the *IFLF.cfg.ecr* file. Once all filter modifications and saving is complete, the application is exited by clicking the **Exit** button. If the current filter settings have not been saved, the user is prompted to save the configuration immediately prior to exiting the application.

3.6.7 System Startup

Startup of the TTA system consists of starting up the TTA low and TTA high side processes running on the TTA low and TTA high platforms respectively.

To start the TTA low side processes, execute the following steps on the TTA low platform as a TTA Administrator:

1. Change the current working directory to the installed TTA directory.

```
% cd <full path to tta_v1.0.2_low>/tta
```
2. Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```
3. Change the current working directory to the TTA *scripts* directory.

```
% cd <full path to tta_v1.0.2_low>/tta/scripts
```
4. Initialize the TTA System by performing the following command and responding to each prompt:

```
% ./TtaInitSys.csh LOW
```
5. Start up the TTA System by executing the following command:

```
% ./TtaSysStartup
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):
running /opt/tta_v1.0.2_low/tta/bin/solaris26/ttalogd
running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgCreate
running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgSend
running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaPrdStatDmn
```

DRAFT

```
running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaGkprIntrfc
```

To start the TTA high side processes, execute the following steps on the TTA high platform system as a TTA Administrator:

1. Prior to starting the TTA High system, the TTA Administrator needs to verify that the Inclusive Field Level Filter file, *IFLF.cfg.ecr*, exists in the *<full path to tta_v1.0.2_high>/tta/config/<hostname>* directory. Perform the following steps to verify that this file exists:

```
% cd <full path to tta_v1.0.2_high>/tta/config/<hostname>
```

Check the contents of the directory by executing the following command:

```
% ls -al
```

If the encrypted version, *IFLF.cfg.ecr*, of the file does not exist in the directory refer to section 3.6.6.2 of this manual to configure field level filters before starting the TTA system.

2. Perform the following commands to initialize and start the TTA High system:

Change the current working directory to the installed TTA directory.

```
% cd <full path to tta_v1.0.2_high>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA *scripts* directory.

```
% cd <full path to tta_v1.0.2_high>/tta/scripts
```

Initialize the TTA System by performing the following command and responding to each prompt:

```
%. /TtaInitSys.csh HIGH
```

Start up the TTA System by executing the following command:

```
%. /TtaSysStartup
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):
running /opt/tta_v1.0.2_high/tta /bin/solaris26/ttalogd
running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgCreate
running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgSend
running /opt/tta_v1.0.2_high/tta/bin/solaris26/KeymapRcvProc
running /opt/tta_v1.0.2_high/tta/bin/solaris26/tta_plugin.SVR4
running /opt/tta_v1.0.2_high/tta/bin/solaris26/SFA
```

DRAFT

3.6.8 System Shutdown

To stop the TTA low side processes, execute the following steps on the TTA low platform system as a TTA Administrator:

Change the current working directory to the installed TTA directory.

```
% cd <full path to tta_v1.0.2_low>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA *scripts* directory.

```
% cd <full path to tta_v1.0.2_low>/tta/scripts
```

Halt the TTA System by performing the following command:

```
% ./TtaSysShutdown
```

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):
running /opt/tta_v1.0.2_low/tta/bin/solaris26/ttalogd
not running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgCreate
not running /opt/tta_v1.0.2_low/ttaCGI/bin/tta/solaris26/TtaPckgSend
not running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaPrdStatDmn
not running /opt/tta_v1.0.2_low/tta/bin/solaris26/TtaGkprIntrfc
```

This will shutdown all TTA process except for the *ttalogd* process. In general this process can remain active. If for some reason, the entire system needs to be halted, perform the above steps and, in addition, execute the following command to terminate the *ttalogd* process:

```
% kill `ps -e | grep ttalogd | awk '{print $1}'`
```

To stop the TTA high side processes, execute the following steps on the TTA high platform system as a TTA Administrator:

Change the current working directory to the installed TTA directory.

```
% cd <full path to tta_v1.0.2_high>/tta
```

Set up the run time environment by executing the following command:

```
% source TTAvars.csh
```

Change the current working directory to the TTA *scripts* directory.

```
% cd <full path to tta_v1.0.2_high>/tta/scripts
```

Halt the TTA System by performing the following command:

DRAFT

% ./TtaSysShutdown

If successful, a message similar to the following will be displayed in the terminal window:

```
TTA v1.0.2 Process Status (Mon Jul 9 09:28:12 EDT 2001):
running /opt/tta_v1.0.2_high/tta/bin/solaris26/ttalogd
not running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgCreate
not running /opt/tta_v1.0.2_high/ttaCGI/bin/tta/solaris26/TtaPckgSend
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/KeymapRcvProc
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/tta_plugin.SVR4
not running /opt/tta_v1.0.2_high/tta/bin/solaris26/SFA
```

This will shutdown all TTA process except for the *ttalogd* process. In general this process can remain active. If for some reason, the entire system needs to be halted, perform the above steps and, in addition, execute the following command to terminate the *ttalogd* process:

```
% kill `ps -e | grep ttalogd | awk '{print $1}'`
```

3.7 Auditing

3.7.1 Levels of Auditing

Three distinct levels of auditing exist within the TTA system: Operating system level auditing, Broadsword Gatekeeper auditing, and TTA auditing. The following paragraphs describe the scope and location of each of these audit mechanisms:

Operating System Level Auditing: Inherent capabilities in the Solaris operating system cause audit records to be written to */var/log/syslog*. The audit records contain detailed information on a variety of low level events occurring on the system (such as processes starting and stopping, user logins and logouts, users entering and exiting privileged roles, modification to user accounts and passwords, etc). This log information can be viewed with standard text editors like vi.

Broadsword Gatekeeper Auditing: At the foundation of the TTA architecture are high side and low side Broadsword Gatekeepers configured for use by TTA. Within the TTA Gatekeepers, Broadsword audits are maintained using a Sybase DBMS which records every Broadsword related message that enters or leaves the TTA High and Low Gatekeeper domains. Operations performed by the TTA Plug-in (queries, and product requests), TTA Package Create (transfer of queries, product requests and keymap updates), TTA Gatekeeper Interface (processing queries and product requests), Keymap Update Daemon, (processing updates) and Keymap Receive (processing updates) are audited. Tools for accessing, reducing, and analyzing the Sybase resident audit records are provided to authorized users through the Gatekeeper User Interface. A detailed description of this auditing capability and use of the Broadsword provided audit access and reduction tools is provided in the Trusted Facility Manual for Broadsword Version 3.1.

DRAFT

TTA Application Auditing: Detailed TTA application-level auditing is implemented within the TTA High side and Low side components. All operations performed by the various TTA Gatekeeper, TTA Plug-in, Security Filtering Application, TTA Package Create, TTA Package Send processes, TTA Gatekeeper Interface, Keymap Update Daemon, and Keymap Receive are audited to create a continuous audit trail describing end to end flow through all components of the TTA high or TTA low system. This currently active log file is located in the `/var/log/syslog` file. The `var/log` directory may likely contain other log files (labeled `syslog.0`, `syslog.1...syslog.n`, etc.) that are not the currently active log file, but contain audit log information.

3.7.2 Audited Information

Figure 3.7-1 depicts a typical TTA audit record and describes each of the fields in the record format. Note that specific system resources related to the event are not described because all TTA events relate to specific TTA processes, rather than system resources such as hard disks, tapes drives, etc.

```
Oct 11 15:56:17 dogwood TTA_PCKG_CREATE[9407]:6:INFO:
ttaadm[1029]:AUDITING:TTAPackage[tta9428.2000101115552683]:
SessionId[9428]: Package Verification Failure,Invalid MD Seal
```

1. Date and time that the audit record was generated
2. Hostname on which the audit record was generated
3. Program generating the event with process ID (in brackets)
4. Message Level Number
5. Message Level Field
6. Person running the program with user ID (in brackets)
7. Event Type
8. TTA Package ID (in brackets)
9. Session ID (in brackets)
10. Event Description

Figure 3.7-1: TTA Audit Record Example

3.7.3 Audited Activities

System level events such as logins, printing, and switch user events, are audited by the Solaris operating system upon which TTA resides.

TTA specific events that are audited include the following:

- **TTA_AUDITING**: An event used to identify a main processing state or condition as it relates to specific packages within the TTA system, (i.e., transaction processing, verification of packages, filtering, moving packages, transferring across security boundaries).

DRAFT

- TTA_SYS_INIT_WARNING: An event that identifies a non-fatal system initialization condition, (i.e., using default values for undefined control variables).
- TTA_DEBUG: An event used to support on-site trouble-shooting or debugging capabilities.
- TTA_ENV_ERR: An event that identifies errors that occur during the TTA process initialization phase (i.e., unable to load environment configuration file, environment variable not being set and unable to use default values).
- TTA_SYS_ERR: An event that identifies errors pertaining to conditions of the TTA system, (i.e., unable to send mail, unable to execute a system command, ftp errors, trying to start a server that is already running, etc.)
- TTA_SYS_INIT_ERR: An event that identifies errors that occur during the initialization of the TTA system, (i.e., unable to open audit log, unable to establish or initialize shared memory, error starting processes, etc.)
- TTA_ACCESS_ERR: An event that identifies an error that pertains to the creation, accessing, and manipulation of files and directories.
- TTA_DECR_ERR: An event that identifies that a decryption error has occurred.
- TTA_ENCR_ERR: An event that identifies that an encryption error has occurred.
- TTA_PCKG_ERR: An event that identifies an error pertaining to a specific package as it is being processed, (i.e., unable to access or process control file contents, security translation errors, unknown or non-supported message types).
- TTA_GKPR_ERR: An event that identifies errors that occur between the TTA system and the TTA gatekeeper, (i.e., error retrieving gatekeeper info, unable to connect to gatekeeper, unrecognizable gatekeeper message type, unable to process gatekeeper message, unable to create, modify, and/or delete sources).
- TTA_MD_ERR: An event that identifies a Message Digest 5 (MD5) validation failure has occurred.
- TTA_DW_ERR: An event that identifies that a Broadword message has failed to pass the exclusive global word tests.
- TTA_FILTER_ERR: An event that identifies that a Broadword message has failed to pass the inclusive field level filter tests.
- TTA_BSWD_ERR: An event that identifies that an error has occurred between the TTA system and the requesting client (i.e., unable to return query responses/products).
- TTA_BSWD_MSG_ERR: An event that identifies an error that has occurred during processing a client's requesting transaction.

DRAFT

- TTA_BSWD_AUDIT_ERR: An event that identifies an error has occurred during updating of the Broadsword audit logs.
- TTA_GUARD_ERR: An event that identifies that the Guard is unable to transfer a TTA package across security boundaries

Audits logs are archived on magnetic media and are to be maintained for a period of 5 years.

3.7.4 TTA Audit System Failure

Due to the importance of maintaining an accurate and complete log of all activities being conducted by the TTA system, a TTA daemon process exists to frequently monitor the continued operation of the *syslog* daemon (*syslogd*). The time interval for this check is configurable, but is preset to be five minutes. If at any time this daemon process detects that the *syslogd* process is not running, two events occur:

1. An email is sent to the ttaAdmins group notifying all of the TTA administrators that the *syslog* error was detected and a system shutdown was issued, and
2. The TtaSysShutdown script is executed to shutdown all TTA processes on the system thus preventing any additional un-audited TTA events.

3.7.5 TTA Audit Reduction

Because of the high volume of information potentially written to the TTA Audit log, audit reduction tools are needed to allow the ISSO to quickly reduce the TTA audit log content down to a set of events pertinent to a specific user, package, or process. The following describes the use of TtaAuditReport, a script that was developed to support TTA audit log reduction and analysis.

This TtaAuditReport script, located in the *<full path to tta_v1.0.2_high_or_low>/scripts* directory, provides the ability to generate a complete trace for a particular tta package id, Broadsword session id or TTA process. The syntax of the command is as follows:

```
% ./TtaAuditReport <value to search for> <log file> [<log report file>]
```

The command takes three arguments:

- | | |
|------------------------------------|---|
| <value to search for> | A mandatory argument containing any string that occurs in the event log such as a known TTAPackageId, Broadsword SessionId or TTA process name. |
| <log file> | A mandatory argument containing the name of the file to search. This file can be the currently active log file (<i>/var/log/syslog</i>), an inactive online log file (<i>/var/log/syslog.1</i>), or a previously archived log file recovered from tape (see section 3.7.6 of this document for archival and recovery instructions). |
| [log report file] | An optional argument containing the name of a file that will be created/overwritten to contain the output of the |

DRAFT

TtaAuditReport script. Note, that if this argument is not provided, the output will be written to stdout (the active window).

The following is an example use of the script as it would be used to search for a TTA package ID (tta8107.2000101716314889) in the active *syslog* file (*/var/log/syslog*) with the output directed to stdout (no third argument is provided):

```
% TtaAuditReport "tta8107.2000101716314889" /var/log/syslog
```

The following Figure 3.7-2 contains an example output generated by the script:

```
-----
Dumping Audit Report to stdout
-----
Oct 17 16:31:49 dogwood TTA_PLUGIN[8131]: 6:INFO
:mikem[1024]:TTA_AUDITING: TTA
Package[tta8107.2000101716314889]:SessionId[8107]: Security Translation
Performed on Message -
719|GCQM|26|TRACE_KEY|tta.1234.123415|QUERY_TYPE|015|THUMBNAILS|Y14|MAX
_HITS|1034|QS|27|BQS_STMT|PRD.CLASS =
"U"605|RC|46|SOURCE_REF|80c50d40:965089257:IPL:96509063020|HIT_LIST|IMG
.ABPP18|HIT_LIST|IMG.IC22|HIT_LIST|IMG.COMRAT21|HIT_LIST|IMG.NCOLS21|HI
T_LIST|IMG.NROWS23|HIT_LIST|KEY.KEYWORD21|HIT_LIST|PRD.CLASS22|HIT_LIST
|PRD.CLEVEL23|HIT_LIST|PRD.CONTROL24|HIT_LIST|PRD.ACCESSID20|HIT_LIST|P
RD.DWNG25|HIT_LIST|PRD.DWNGEVENT23|HIT_LIST|PRD.PRODFMT21|HIT_LIST|PRD.
ONAME27|HIT_LIST|PRD.DATECREATED26|HIT_LIST|PRD.PRODUCERSE26|HIT_LIST|P
RD.PRODCRTIME23|HIT_LIST|PRD.RELEASE21|HIT_LIST|PRD.TITLE24|HIT_LIST|PR
D.NUMFILES29|HIT_LIST|IMG.FILE_NUMBER_I24|HIT_LIST|IMG.FILE_NBR22|HIT_L
IST|IMG.NBANDS25|HIT_LIST|PRD.PRODFSIZE

Oct 17 16:31:49 dogwood TTA_PLUGIN[8131]: 6:INFO
:mikem[1024]:TTA_AUDITING: TTA
Package[tta8107.2000101716314889]:SessionId[8107]: Creating Client
Message Package

.
.
.
```

Figure 3.7-2: TTA Example Audit Log Reduction Output

If argument 3 is specified, the TtaAuditReport will write the output to a file rather than to the screen. If the administrator chooses this option, TtaAuditReport will first check for the existence of the output file and prompt the user to determine whether to overwrite this file or not. By pressing <Ctrl -c> the user will exit the TtaAuditReport script with no

DRAFT

action done. By pressing <return> the user will confirm the overwrite, and the script will proceed with overwriting the file. The user can then view the file using any UNIX text editor such as vi.

3.7.6 TTA Audit Archival and Restoration

Due to the high volume of information potentially written to the TTA Audit logs and the requirement in DCID 6/3 that audit records be maintained for a period of 5 years, it will be necessary to periodically archive the non-active audit log file to tape and remove the archived files from the system. The following describes the steps necessary to perform TTA audit log archival.

Archival to Tape:

From a terminal window the TTA administrator should *su* to root by entering the following command and, when prompted, entering the root password.

```
# su root
```

Change directory to where the *syslog* file(s) exists by executing the following command.

```
# cd /var/log
```

Verify you are at the correct directory location by executing the following command:

```
# pwd
```

The current location is echoed to the screen and should be:

```
/var/log
```

Obtain a directory listing by issuing the following command:

```
# ls -l
```

A listing of the */var/log* directory should be shown on the screen and look something like the following:

```
drwxr-xr-x  2 root   sys      512 Oct 14 04:05 .
drwxrwxr-x 19 root   sys      512 Apr 3 2000 ..
-rw-----  1 root   sys        0 Mar 23 2000 authlog
-rwxrwxrwx  1 root   root     172 Mar 23 2000 sysidconfig.log
-rw-r--r--  1 root   other   694572 Oct 17 18:02 syslog
-rw-r--r--  1 root   other  2520536 Oct 14 03:56 syslog.0
-rw-r--r--  1 root   other  2029293 Oct 7 04:05 syslog.1
-rw-r--r--  1 root   other   686486 Sep 30 04:02 syslog.2
-rw-r--r--  1 root   other    273 Sep 21 12:52 syslog.3
```

Note: In this listing, there are five files of interest to the administrator, the currently active log file (*syslog*) and four inactive log files (*syslog.0*, *syslog.1*, *syslog.2*, *syslog.3*). **The currently active *syslog* should never be archived to tape. Only inactive log files should be archived.**

DRAFT

To archive an inactive log file such as *syslog.3*, insert a non-write protected tape (8 mm or 4mm depending on tape device) into the tape device connected to the TTA host. Note, the following steps overwrite any data that may already be on the tape. After a tape has been loaded into the tape device, execute the tar command to write the desired file of the *syslog* to tape. The following describes the syntax of tar command:

```
# tar cvf <device name> <file to archive>
```

<device name> Name of a valid archive device.

<file to archive> Name of the log to be archived to tape.

Much more information describing the *tar* command is available via online manual pages simply by issuing the “man tar” command. The following is an example archive command to write the *syslog.3* file to the tape device /dev/rmt/0:

```
# tar cvf /dev/rmt/0 ./syslog.3
```

The *syslog* file is written to tape. Information should be written to the screen indicating that the *syslog* file is the only file written to the tape device. When the tar command is complete, the user should verify that the tape does in fact contain the desired file. This is done by performing the following command, where /dev/rmt/0 is the device name:

```
# tar tvf /dev/rmt/0
```

The command should result in a listing of the file(s) in the archive (in our example, file *syslog.3*). With the correctness of the archive verified, the user should now eject, write protect, label, and secure the tape in a secure storage area approved for protecting the information on the tape at the security level of the system on which it was generated. A recommended practice is to label the tape with the type of archive, system name, and date time stamp of the first and last entry in the archived log file or files:

Archive Type: TTA Audit Archive

System : TTA_High

Date Time Span : Oct 10 11:42:09 - Oct 17 16:31:49

The date time span information is easily obtained by executing Unix head and tail commands on the archived file, and noting the first and last date times associated with the events in the log. Once the tape has been labeled and secured, the administrator may choose to remove the file from the online directory by issuing the following command:

```
# rm syslog.3
```

Where *syslog.3* is the name of the file to be removed. The archive is now complete.

Recovery from Tape:

After a log has been archived to tape, it may be necessary to view the log to conduct security related analysis of its contents. To do this, the archived log must be recovered from tape into an online file. Once online, the audit reduction tools described in section 3.7.5 can be freely applied against it. The following describes the steps necessary to perform TTA audit log recovery from tape.

DRAFT

From a terminal window the administrator must *su* to root by entering the following command and, when prompted, entering the root password.

```
# su root
```

Create a designated directory such as *<full path to tta_v1.0.2_high_or_low>/data* to store the recovered *syslog* files. Change directory to where the *syslog* file(s) is to be placed by entering the following command:

```
# cd <full path to tta_v1.0.2_high_or_low>/data
```

Make a directory in that location identifying the date and time span of the recovered archive. The start dates and end dates should appear on the archive tape (i.e., Oct 10 11:42:09 - Oct 17 16:31:49). The following command would be used to make the appropriately named directory:

```
# mkdir "Oct 10 11:42:09-Oct 17 16:31:49"
```

Next, change directory to the newly created directory by entering the following command:

```
# cd "Oct 10 11:42:09-Oct 17 16:31:49"
```

Verify you are at the correct directory location by executing the following command:

```
# pwd
```

The current directory location is echoed to the screen. Next, insert the archive tape into the tape device

To recover an inactive log file such as *syslog.3*, insert archive tape (8 mm or 4mm depending on tape device) into the tape device connected to the TTA host, and execute the tar command to write the desired file from tape to hard disk. The following describes the syntax of tar command where *<device name>* is the name of a valid archive device:

```
# tar xvf <device name>
```

Information will be written to the screen indicating that the *syslog* file(s) has been extracted from tape and placed onto the disk. When the tar command is complete the user should verify that the disk directory contains the desired file. This is done by performing the following command:

```
# ls -l
```

The command should result in a listing of the file(s) in the directory (in our example, file *syslog.3*) which is now located on the disk.

The recovery is now complete. The audit reduction tool described in Section 3.7.5 of this report can now be applied against the recovered log file by using the full path to the log file as the *<log file>* parameter in the *TtaAuditReport* command.

DRAFT

3.8 Marking and Labeling

3.8.1 Hardware, Storage Media, and Hardcopy Output

All computer hardware (CPUs, monitors, etc), storage media (hard disks, tapes, removable disks, etc.) and hardcopy outputs comprising or produced from the TTA systems will be labeled and handled at the classification level of the related system, i.e. TS/SCI for the TTA high system and US Secret for the TTA low system. Sanitization and destruction of these components will be performed by authorized personnel in accordance with all site specified procedures.

3.9 Software Security Procedures

3.9.1 Procurement

The TTA systems are closed, special purpose systems. Thus it is not necessary for site administrators to install and execute any additional software on the systems. All operating system and TTA software upgrades and patches will be performed in coordination with the Broadsword/TTA PMO, security accreditors, and local ISSM/ISSO personnel.

3.9.2 Protection from Viruses and Malicious Code

The TTA systems are closed, special purpose systems with all standard Solaris remote access services either eliminated or constrained thus the risk of virus and/or malicious code introduction is significantly reduced. The executables, data files, scripts and configuration files controlling TTA functionality are protected from access and modification by non-privileged users by Solaris. Bi-directional virus detection is performed on all files being transported through the ISSE Guard across security domains via the TTA systems. Should computer viruses or malicious code be detected on TTA systems, they should be immediately shutdown, the site ISSMs and ISSOs notified, and site specified incident reporting and response process initiated.

3.9.3 Maintenance

To support maintenance and emergency recovery of the TTA systems a separate version of the Solaris operating system, the Broadsword gatekeeper installation software and the TTA installation software (all typically supplied on CD-ROM) will be stored on-site.

3.10 Media Movement

All information (files, audit logs, executables, printed outputs, etc.) obtained from the TTA systems in various media (hard disks, removable tapes, floppies, paper output, displays, etc.) will be labeled and handled at the classification level of the system it was produced from. Transportation or release of this information outside of the secure facility will be performed by authorized personnel in accordance with all site specified procedures. Downgrade and release of this information will be performed by authorized release authorities in accordance with all site specified procedures.

3.11 Hardware control

The hardware on which the TTA system resides is standard commercially available hardware, thus no special hardware control considerations are imposed by the TTA system. Any hardware control related activities (including system transport, relocation, maintenance, and acquisition) are to be performed in accordance with the hardware control policy and procedures as defined by the site.

3.12 Web Protocol and Distributed/Collaborative Computing

The TTA system has no distributed or collaborative computing aspects to its operation. Since the TTA system software runs on top of a Broadsword Gatekeeper configuration specific web protocol aspects of its behavior are inherited from the Broadsword Gatekeeper upon which it is based. For a discussion of these issues refer to the Web Protocol and Distributed/Collaborative Computing section of the *Trusted Facility Manual for the Broadsword Gatekeeper*.

4 BACKUP POLICY AND PROCEDURES

It should be noted that the correct and secure operation of the TTA system is dependant on the proper installation and configuration of many components of the architecture including the Solaris operating system, Broadsword Gatekeeper and TTA system software. The following instructions describe creation of a backup tape for the TTA system software portion only. If it is necessary to do a complete restoration of the entire TTA platform instructions should be followed for reinstalling/recovering the operating system, and Broadsword in accordance with Solaris, and Broadsword instructions prior to recovering the TTA software from backup tape.

To backup of the TTA software, including its various configuration files, to removable media the following steps are performed:

1. Insert a non-write protected tape (8 mm or 4mm depending on tape device) into the tape device connected to the TTA host being backed up. Next, perform the following tar command as root substituting a full pathname for the parameter in <>. Note: the following command will overwrite any data that may already be on the tape.

tar cvfp <full path to tta_v1.0.2_high_or_low >

2. Once the tar command is complete, remove the TTA backup tape from the system's tape drive, label it with the contents and the date the backup was created, write protect it, and place it in a secure storage location.

5 RESTORATION POLICY AND PROCEDURES

Note: The following instructions describe recovery of a backup tape for the TTA system software portion only. If it is necessary to do a complete restore of the entire TTA of TTA platform instructions should be followed for reinstalling/recovering the operating system, and Broadword in accordance with Solaris, and Broadword instructions prior to recovering the TTA software from backup tape.

To recover the TTA system backup from a tape created in accordance with the backup instructions described in Chapter 4 of this manual the following steps are performed:

1. Verify and if needed recreate the uppermost level TTA directory. Assuming that the TTA system was originally installed in the /opt directory with the name `tta_v1.0.2_high`, the following commands create the uppermost TTA directory:

```
# cd /opt
```

```
# mkdir tta_v1.0.2_high
```

2. Execute the following command to change the ownership of the newly created install directory to `ttaadm` and the group to `tta`:

```
# chown ttaadm:tta tta_v1.0.2_high
```

3. Execute the following command to change the permissions of the newly created install directory:

```
# chmod 777 tta_v1.0.2_low
```

4. Place the TTA backup tape in the system's tape drive and execute the following command:

```
# tar xvfp /dev/rmt/0 /opt/tta_v1.0.2_high
```

5. Once the tar command is complete, remove the TTA backup tape from the system's tape drive and return it to a secure storage location.

6 KNOWN VULNERABILITIES AND RISK MITIGATION APPROACH

A discussion of the potential vulnerabilities of the TTA system is provided in section 2.1 of this manual. Chapters 2 and 3 describe the various capabilities built into the TTA system to reduce the likelihood and mitigate the risks associate with these vulnerabilities.

DRAFT

APPENDIX A EXCLUSIVE GLOBAL FILTER EXPRESSIONS

The following list provides examples of expressions which can be placed in the *dirty_word.cfg* file and the matching criteria that each of those expressions will generate when interpreted as an Exclusive Global Filter.

Examples	Matches
-top secret	top secret
-(t T)op (s S)ecret	top secret, Top secret, top Secret, etc.
-[tT]op [sS]ecret	top secret, Top secret, top Secret, etc.
-top secret	top, secret
-(top very) secret	top secret, very secret
-top secre(ts)*	top secre, top secrets, top secretsts, etc.
-top secrets+	top secrets, top secretss, etc.
-(top)* secret	secret, top secret, top top secret, etc.
-t.p secret	top secret, tap secret, t5p secret, etc.
-t\.p secret	t.p secret
-secret ab	secret ab
-secret (a c)	secret a, secret c
-secret [ac]	secret a, secret c
-secret a secret c	secret a, secret c
-secret [a-c]	secret a, secret b, secret c
-secret ^[a-c]	secret d, secret 3, secret f, secret M
-secret [a-c][d-f]	secret ad, secret ae, secret be, secret cd, etc.
-top secret\$	top secret - at end of line
-\(top\) secret	(top) secret
-\([tT]op\) secret	(top) secret, (Top) secret
-\(\([tT]op\) \)* secret	secret, (top) secret, (Top) secret, (top) (Top) secret, etc