White Paper

Trusted Computing—The SGI® Solution

1.0 Introduction

The SGI family of graphics workstations and compute servers has become the platform of choice for demanding technical computing applications. Many users and developers in these fields require a new dimension to their 3D computing environment: security. To meet the needs of security-sensitive users and to maintain the leading position for 3D graphics and visual imaging, SGI has developed the Trusted IRIX™ operating system. SGI has the history of trusted systems expertise and the tradition of service to the federal marketplace necessary to make a solid commitment to this optional add-on to the IRIX® 6.5 operating system. Trusted IRIX allows users who must maintain security to use all of the features that made SGI their first choice for 3D computing.

Leading-edge graphics technology and a tradition of service in the federal marketplace set the SGI solution apart from those offered by all other vendors. Trusted IRIX supports the entire range of industry-leading SGI hardware and software, enabling the secure government or commercial site to take advantage of the SGI solution.

This document is a comprehensive technical overview of Trusted IRIX. It describes in detail the important features of a trusted operating system and the specific implementation within Trusted IRIX. Trusted IRIX is an optional add-on to the full-feature set of standard IRIX as well as a set of security features to satisfy the most demanding requirements. Because Trusted IRIX is designed to be fully compatible with standard IRIX, it provides a usable and accessible trusted software platform. Trusted IRIX supports the full SGI hardware product line and third-party application software, including networking and a native X Window System. Trusted IRIX is also a high-performance system, with less than 5% performance degradation compared with standard IRIX.

2.0 What Is a Trusted System?

Operating systems that attempt to provide a secure environment for the development and storage of sensitive information are known as trusted systems. In an abstract sense, no system is ever perfectly secure from harm, so we prefer the term trusted rather than secure. A trusted system can be thought of as any system that provides two important features:

- The system allows all users to do their ordinary and necessary work without difficulty
- The system enforces the security policy deemed by the management to be appropriate to the site

The first criterion is the most important. If users are unable to do their ordinary and necessary work, they will either circumvent the security measures or not use the system at all. In either case, the trusted system is useless. Many users are concerned that they will not be able to do their work in a secure environment. Proper planning leads to a situation that minimizes denial of access and resources to the users. Ideally, the users should be able to perform all their tasks and never see the trusted features of the operating system.

To meet the second criterion, the system must have adequate security features to enforce the site security policy set forth by the management. Presumably, the decision to purchase a B1-level trusted system has been made after research and consideration, and it is clear that this level of security is necessary at the site.

3.0 Definition of Trusted IRIX

The Trusted IRIX operating environment, an extension of the IRIX operating system, is no longer a separate operating system under IRIX 6.5. IRIX is the SGI implementation of the UNIX® System V operating system. Trusted IRIX is a separately purchased add-on product that was developed to conform to standard Trusted Computer Security Evaluation Criteria (TCSEC) B3 feature set, but with the assurance of security at the B1 level. A standard installation of IRIX 6.5 is a C2-level deployment. At this level, IRIX features:

- Identification and authentication
- Capability-based privilege mechanism
- Superuser-based privilege mechanism
- Discretionary access control
- Object access control list
- Hardware object scrubbing
- Activity audit trailing

A B1-level deployment of IRIX is achieved by installing Trusted IRIX. Trusted IRIX confers the additional feature of mandatory access controls (also known as mandatory object sensitivity/integrity).

The B1 and C2 levels fall within a range of security levels specified by theTCSEC Standard (also known as the Orange Book) from C1 (least secure) to A1 (most secure). The defined levels of security are C1, C2, B1, B2, B3, and A1. The B1 rating requires several features not present in standard UNIX systems and requires review and modification of existing codes. Added features include improved user identification and authentication procedures, audit records of all system activity, and more stringent access controls on files and devices.

4.0 The Importance of Trusted IRIX

In the near future, most government workstation procurement contracts will require trusted operating systems. Already, a significant percentage of military and Department of Energy purchase requisitions are requiring C2- or B1-level security. The United States government is committed to trusted operating systems.

The National Computer Security Center was established by the Department of Defense to evaluate and certify hardware and software for use by the federal government. The NCSC also has become the primary developer and distributor of standards of operating-system security. NCSC TCSEC standards are recognized throughout the industry as the preeminent definitions of trusted systems. Trusted IRIX meets or exceeds all TCSEC standards for a B1-level trusted operating system. In addition to Orange Book requirements, Trusted IRIX is compliant with Department of Energy standards. These additional standards include password generation, automatic password aging, and some specific audit event types.

Because it provides a full IRIX feature set as well as security enhancements, Trusted IRIX meets the market demand for trusted systems. The B1 evaluation in progress by the NCSC gives the customer assurance that the product is indeed trustworthy. Until the product is formally placed on the NCSC Evaluated Products List, documentary evidence for the product is available to assist site-specific certifications.

5.0 The Purpose and Value of Trusted IRIX

Trusted IRIX is designed to address the three fundamental issues of computer security: policy, accountability, and assurance. By fully addressing these areas, the system becomes a trustworthy base for secure development and operation. Since the specific features provide the mechanisms necessary for security, little must be trusted beyond the system itself. When application programs are in use on the system, there is a reasonable certainty that the applications will be free from corruption and safe from intruders. All features of Trusted IRIX are designed to support the B1 security philosophy. Each aspect of the system reflects a requirement set forth by the NCSC.

6.0 A Usable Trusted System

The most important feature of a trusted system is usability. If a system is not usable, security features are wasted. The security features in Trusted IRIX are for the most part transparent to the user and, when visible, are convenient and do not disable other system features.

Trusted IRIX has implemented all the required security features for a B1 operating system and maintained the familiar interface and feature set that SGI customers have come to expect. Trusted IRIX systems support the client/server-computing model and can interoperate with standard IRIX systems. Trusted IRIX supports the entire range of third-party applications available for SGI computers.

SGI is committed to the Trusted Systems Interoperability Group, and Trusted IRIX will be compatible with all major trusted systems. SGI is actively contributing to the POSIX 1003.6 standard.

7.0 A High-Performance Trusted System

Trusted IRIX runs on all current SGI hardware platforms with minimal performance degradation. The new Trusted IRIX system runs on all SGI hardware with no more than a 5% performance impact compared to IRIX 6.5. Trusted IRIX also allows the system administrator to limit disk-space usage of disk-intensive features such as the System Audit Trail.

8.0 A Full-Feature Trusted System

Trusted IRIX incorporates the full B1-level feature set standardized by the NCSC, with further security enhancements, such as integrity labels and trusted multilevel networking, described in detail in this document. Trusted IRIX includes a host of application programs, such as REACT™ real-time support and Workspace visual-command shell.

The trust in Trusted IRIX depends on security features and assurance. Assurance of security is based on the fact that SGI is under evaluation for the B1 security rating from NCSC. The security features in Trusted IRIX are described in the NCSC B1 criteria. These criteria include:

- Identification and authentication:
  Users must adequately identify themselves to the system with a login account name and a secret password before being granted access to any system resources
- Audit accountability:
  The actions of all users on the system must be subject to audit to make a record of all system activity
- Object reuse:
  Mechanisms must ensure that no trace of a used object is left in any publicly readable state, such as in memory or on the screen
- Labeling:
  The system must associate a label with every subject and object for the purposes or mandatory access control

- Mandatory access control (MAC):
  The label of every subject and object on the system must indicate a level of clearance; based on the level of clearance, access to objects by subjects can be controlled by the operating system
- Discretionary access control (DAC):
  The owner of any object must be able to control access to that object within the trusted system

The implementation of each of these features in Trusted IRIX is described in detail in the following sections.

9.0 Trusted IRIX Security Features

The distinguishing difference between trusted systems and nontrusted systems is the security-enhanced feature set. For B1-level systems, this feature set includes four main components. These components are improved identification and authentication of users, auditing, object reuse, and access control (MAC and DAC). Also discussed are the X Window System and networking implementations for the trusted environment. Each component feature is described in detail below.

Every trusted system has a trusted computing base (TCB). The TCB is the operating-system program itself and the commands, utilities, tools, and system files that are known to be secure. This set of files and programs is the "trusted" part of a trusted system.

Within the TBC, there are subjects and objects. A subject is any active force on the system, such as a user's shell process, the audit daemon, or the operating system itself. An object is any passive resource on the system, such as a text file, a page of memory, or a piece of system hardware.

10.0 Identification and Authentication

The identification and authentication (I&A) mechanism controls user access to the system. In common terms, the I&A mechanism is the login procedure. This subsystem is always active if the system is running, and it is impossible to have any contact with the system without first logging in through the I&A system.

All login attempts are audited by the system with special attention paid to unsuccessful login attempts. The improved I&A facilities of Trusted IRIX allow the administrator to be certain that the people on the system are authorized users and that private password integrity is maintained to the highest possible levels.

11.0 Passwords under Trusted IRIX

Under Trusted IRIX, all passwords are stored in a shadow password file, unavailable for viewing by users. As with standard IRIX, passwords are stored in encrypted form. The threat from a visible encrypted password file is that an intruder may encrypt a number of possible passwords and attempt to compare them with the real encrypted passwords. Under Trusted IRIX, the /etc/passwd file does not contain the encrypted password; only the shadow password file contains that information.

In response to Department of Energy extensions to the B1 requirements, passwords can be generated automatically for the users under Trusted IRIX. System administrators can configure the system to require this feature for every password change, or it can be an option for the user. The complexity, length, and character combinations required of passwords can also be configured. For example, it is possible to require users to mix control characters into their passwords. It is also possible to check and reject technical words associated with computers or the current project. System administrators can also require passwords to be changed on a regular basis.

12.0 Multilevel Login

Individual users may have a range of security levels available that have been predetermined by the administrator. The user is not always required to log in at the highest assigned level, thus allowing the flexibility to log in at a level appropriate for a given task. After successful login has been established, the user may change the clearance of his or her process during the course of the login session. When this happens, all open file descriptors are closed and all objects cleared to prevent declassification or violation of the security policy. All changes of clearance are audited.

13.0 Shadow Password File

Encrypted passwords are stored separately from other user-identification information. This separate location is hidden from normal user access, so the process of a systematic "dictionary encryption" hunt for a password is precluded. User-clearance information is also stored in a hidden or shadow file.

14.0 System Audit Trail

A foundation of Trusted IRIX is the system audit trail. The system audit trail provides a means for the system administrator to oversee each important event taking place on the system. The audit trail is useful for tracking changes in sensitive files and programs and for identifying inappropriate use of the system.

The audit trail is generated by an additional code in the operating-system kernel that notes specific important events, such as file creation, file changes, file removal, invocation of programs, and the login and logout events.

The audit subsystem allows the administrator to create a dynamic record of the system's activity. This record allows the administrator to hold each user strictly accountable for his or her actions. The audit system is completely configurable at any time by the audit administrator.

Audit information must be carefully gathered and protected so that actions affecting security can be traced to the responsible party. Trusted IRIX records the occurrences of security-relevant events in an audit log. For each event audited, the system records the date and time of the event, the initiating user, the type of event, the success or failure of the event, and the names and security classifications of the files or programs used. The auditing process is transparent to the user.

15.0 Preselected Audit

The system administrator has the capability to select the audit events to be recorded. This configurability allows the system administrator to tailor the audit trail to include only those events relevant to the specific site. This minimizes the disk usage and general system overhead demanded by the audit trail. Fifty-two separate audit categories are implemented in Trusted IRIX. Using these categories, the following kinds of general events may be audited:

- User login and logout
- Access to a file or resource denied due to enforcement of access control
- Access to a file or resource failed due to nonexistence of the resource
- Changing of directories via cd (1)
- Opening, closing, reading, and writing of files
- Changing DAC permissions of files
- Removal and creation of files
- Mounting of filesystem
- Mounting of NFS filesystems
- Process creation via exec (2)
- Process creation via fork (2)
- Process exit
- Creation of pipes
- Reading and writing process address space
- IPC activities
- Socket activities
- Setting the system clock
- Setting the system hostname
- Setting the system host ID
- Setting the system domain name
- Use of superuser privilege
- Use of audit trail-related commands
- Use of I&A-related commands
- Modification of special system data files

The system administrator can choose any storage location for audit records. The records can be stored in files that are automatically emptied and reused, or they can be saved and periodically removed to long-term storage on tape. This flexibility allows individual sites to set policies concerning the use of computing resources.

16.0 Audit Reduction and Intuitive Interpretation

The administrator can perform audit reduction and interpretation through the use of the sat_reduce (1M), sat_interpret (1M), and sat_summarize (1M) commands. These utilities allow the auditor conveniently to search the audit log for desired activities.

17.0 Object Reuse Policy

To preclude recovery of data after a deletion, display memory and long-term data storage are subject to an object reuse policy and implementation. For example, all system memory is always automatically cleared before it is allocated to another program. Surrendered disk space is also cleaned prior to reallocation.

18.0 Mandatory Access Control

Mandatory access control is at the heart of a trusted system. This access control allows the administrators to set up policies and accounts that will allow each user to have full access to the files and resources he or she needs, but not to other information and resources not immediately necessary to perform the assigned task. The access control is called mandatory because the system will not allow the creation of files or user accounts without the attribute necessary to impose the access control. Also, under MAC, access permission cannot be passed from one user to another, as under traditional UNIX systems that only use discretionary access control, which work together to precisely control system access.

Under Trusted IRIX, mandatory access control is divided into two interrelated subsystems: mandatory sensitivity and mandatory integrity. The access-control enhancements to Trusted IRIX allow the administrator

to set up levels of clearance and related categories of files and other resources and to assign each user a clearance (or range of clearances). Through this system of access controls, the administrator can tailor a user's environment so that the particular user has access only to those files and resources he or she needs to complete required tasks. In the event of a breach of that user's account, the unauthorized user has access to very little of the site's protected information. Each label used for access control has two parts: the sensitivity label and the integrity label. The following diagram shows the components of a label:

Sample Label Structure

Label Name	
Sensitivity Level	Sensitivity Categories
Integrity Grade	Integity Divisions

19.0 Sensitivity Label Components

Sensitivity labels define the classification of files and resources and the clearance level of users. A sensitivity label is composed of a sensitivity level and possibly some number of sensitivity categories.

There are 256 hierarchical sensitivity levels available for the administrator to create security classifications. In a commercial environment, this label attribute could be used to classify, for example, levels of a management hierarchy. Each file or program has one hierarchical sensitivity level. A user may be allowed to use several different levels, but only one level may be given at any given time.

There are 65,000 sensitivity categories available for files and programs. For example, categories could include information sorted by subject matter such as geography, demography, and astronomy. Each file or user can be a member of any number of categories or belong to none at all.

20.0 Integrity Label Components

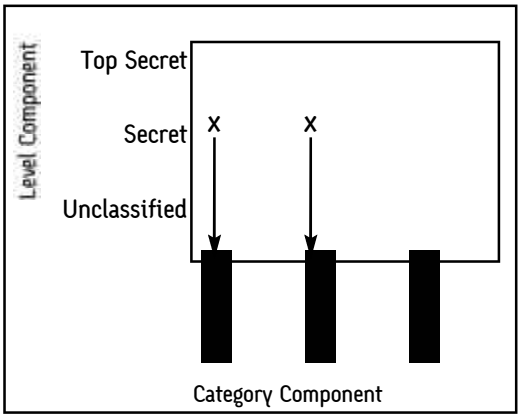
While the sensitivity labels identify whether a user is cleared to view certain information, integrity labels identify whether data is reliable enough for a specific user to see. An integrity label is composed of an integrity grade and some number of integrity divisions.

There are 256 hierarchical grades to classify the reliability of information. For example, data could be classified as an unreliable rumor or as an absolute, confirmed fact.

There are 65,000 divisions available to classify information based on its source. The source implies the probable integrity of the data. For example, sources of data could include the Canadian government, the U.S. government, CBS News, and Hearst Corporation publications. In the commercial environment, data sources could include trade shows, press releases, conversations, and Dataquest.

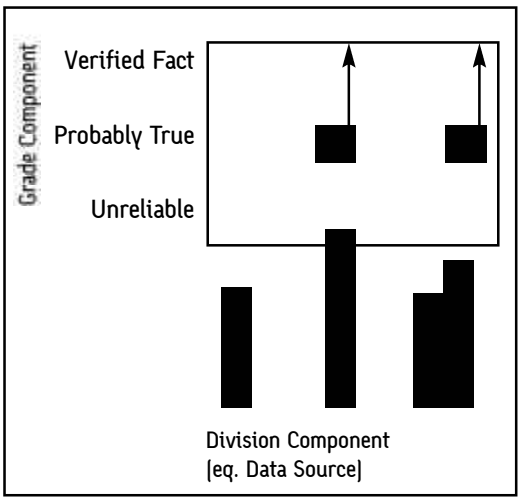
The following diagrams show the relationship between sensitivity levels and categories and between integrity grades and divisions:

Sensitivity Label Components



User has access to files labeled as Project X or Y categories with clearance at Secret and below. User has no access to Project Z or to Top Secret information in any category.

Integrity Label Components



User may access any information from the DOE document, and any information from the Canadian Government. User has no access to Information from the NY Times or to any unreliable data.

21.0 Other Access Control Features

Further access control features of interest include label name and flexibility, superuser protection, MAC protection of passwords, and an object reuse policy. These features are explained below:

21.1 Label-Name Flexibility

Label names are configurable so that specific sites can control naming conventions to meet their special requirements. For example, the site administrator has control of name length and could use non-English names, if desired.

21.2 Protected Superuser

The superuser (root) is not exempt from mandatory access control measures. The system therefore provides double protection against the possibility of inappropriate superuser influence.

21.3 MAC-Protected Passwords

Access to encrypted password files and user-clearance data is under mandatory control.

21.4 Discretionary Access Control

Discretionary access control is the standard UNIX system of permission bits for the user, the group, and the public (all users on the system). DAC permissions are defined by the user who owns the file in question. For example, if a user has a personal file in his or her home directory, that user can set the DAC permissions to allow no other users on the system, save only the root, to view, copy, or edit that file. DAC permissions are changed via the unmask (1) command. The superuser (root) has the power to override discretionary access control.

Thus, to gain access to a file that was created by another user, a user not only must have the proper MAC clearance, but also must have set the DAC permissions on the file to allow others to access it. Typically, DAC permissions would be set to allow access on all but personal files.

22.0 The X Window System under Trusted IRIX

Trusted IRIX supports an X Window System implementation consistent with standard IRIX release 4.0 (a native X implementation). All SGI-supported X and Motif applications run without modification on Trusted IRIX. Trusted IRIX windows are monolabel windows with label display and are subject to audit.

23.0 Networking under Trusted IRIX

SGI customers expect a trusted, graphics-rich environment with compatible networking. The NCSC Orange Book standard for B1-level security does not cover networking, but Trusted IRIX includes support for trusted networks and other networks currently in use.

Given the constraints of assurable security, Trusted IRIX provides trusted multilevel (TML) TCP/IP networking between Trusted IRIX systems and other trusted systems that support the Commercial Internet Protocol Security Option (CIPSO), and monolabel TCP/IP networking to systems that do not support TML networking. This networking takes place using standard Ethernet connections.

24.0 Networking Standards Supported by Trusted IRIX

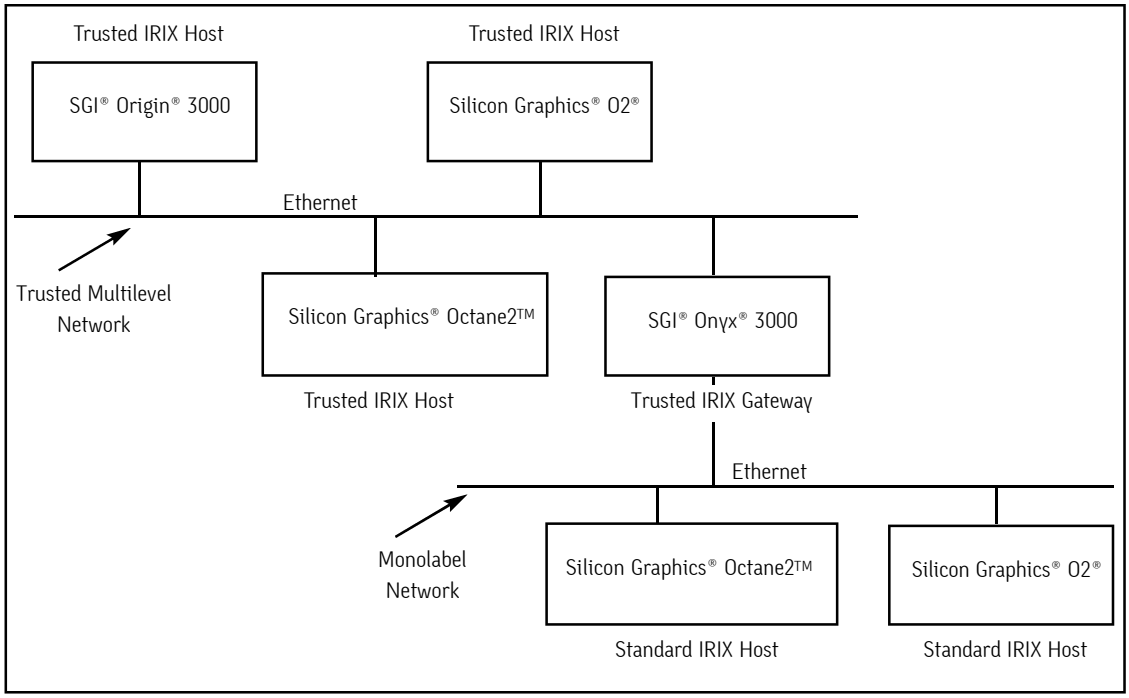
Trusted IRIX supports the Internet Protocol Security Option-Basic Security Option (IPSO-BSO, formerly called RIPSO), CIPSO, and specific extensions to the networking environment permitted by CIPSO for mandatory integrity support.

25.0 TML and Monolabel Networking

Between systems running Trusted IRIX and other systems that support CIPSO, labels may be exchanged freely over the network using the TCP/IP protocol. The appropriate security field in the IP header is used to transport the label. Trusted IRIX also supports trusted networking on networks where security labels are not expressed in IP security options. Trusted IRIX labels all information imported from such networks with a single configurable label and allows only information with the same label to be exported to such networks. The diagram on page 8 illustrates a possible networking scenario in which Trusted IRIX hosts a TML, a gateway machine, and monolabel networking to other IRIX hosts.

26.0 NFS

To provide a full networking feature set, Trusted IRIX uses an enhanced version of the NFS filesystem sharing protocol that allows labels to be maintained across the network. Trusted IRIX maintains the standard NFS file format, using a separate file for labels. Since the file format is maintained, NFS is transparent on Trusted IRIX systems.



Sample Network Including Trusted Multilevel and Monolabel Networks

27.0 Data Import/Export Restrictions

NCSC B1-level security standards indicate that label information must be preserved when files are placed on magnetic storage media, such as tapes. Trusted IRIX tape utilities have been modified to include this feature.

Additionally, B1 standards specify that all paper output must be marked with the label of the information printed. Trusted IRIX line printer software has been modified to add this feature.

28.0 Documentation

Complete System Administrator and user documentation is included with Trusted IRIX. Manual pages are available for all new commands, utilities, and system files. Trusted IRIX shares the IRIX 6.5 documentation and adds a book of specific information about the trusted features.

29.0 Differences between Trusted IRIX and IRIX

Experienced IRIX users will notice some differences between Trusted IRIX and the standard IRIX operating system. The first difference most users see is in the login process. Under Trusted IRIX, the user is asked not only for the login name and password, but also for a preferred security label. However, the most important difference between Trusted IRIX and standard IRIX is mandatory access control. The MAC label on the login shell determines what files and other objects may be used.

30.0 Security Improvements over Traditional UNIX Systems

In traditional UNIX systems, the ability to use security relevant commands is based on one of two considerations: whether the user has execute permission on the program and whether the user ID of the invoking user is root (process has effective user ID 0).

This philosophy has two important side effects. First, root has complete control of the system because all kernel operations and most subsystem operation allow root total access. Second, administrators are forced to share passwords associated with system administration, because each administrator needs to log in to (or use su (1) to enter) the root account in order to perform administrative actions.

The first side effect means that penetrating the root account opens the entire system to the penetrator and that duping an administrator logged in to the system as root into running a malicious program opens the entire system to the program. Many documented and undocumented UNIX system penetrations have resulted from perpetrators guessing or otherwise obtaining the root password or mounting a Trojan horse attack that causes a process with effective user ID root to run the penetrator's program.

The trusted system attempts to reduce the potential of a root program running a Trojan horse by reducing the number of commands that require the invoking user to be logged in as the root. Such command authorizations have mechanisms that allow them to perform system calls that require privilege even though the invoking user is not root. The auditor and administrator accounts have been created to reduce the exposure of the root account.

31.0 Conclusion

With the introduction of Trusted IRIX, SGI delivers a usable, accessible, secure environment to the technical and scientific visual-computing community. SGI is sensitive to customer needs for leading-edge visual computing, driven by government contract requirements. SGI has a demonstrated history of trusted systems experience and a continuing tradition of service in the federal marketplace. Trusted IRIX is the response to government requirements that proves SGI's continued commitment to full-featured, standards-based, state-of-the-art, trusted visual processing.

Corporate Office
1600 Amphitheatre Pkwy.
Mountain View, CA 94043
(650) 960-1980
www.sgi.com

North America 1(800) 800-7441
Latin America (52) 5267-1387
Europe (44) 118.925.75.00
Japan (81) 3.5488.1811
Asia Pacific (65) 771.0290

3185 (12/01) J13212