2.0 SECURITY REQUIREMENTS

This section addresses the security requirements applicable to the DGSA and the process by which organizations can identify the specific security requirements of their missions. Section 2.1 summarizes the DGSA security policy. Section 2.2 describes the DGSA security requirements. Section 2.3 discusses the DGSA derived security requirements needed to support multiple security policies.

An *information system* is a collection of information processing and communications components, and the environment in which they operate, that is used to support the operations of one or more missions. A *security policy* pertains to a mission and is based upon the threats to the means by which that mission is accomplished. A security policy (or, in a more general sense, a collection of security polices) documents the security requirements to be placed upon resources used by an organization. These security requirements express, for the information system personnel, the user organization's desired protection for its information and other system resources.

A security architecture designed to meet a specific mission's security requirements defines the security services and mechanisms and allocates them to components of the mission's information system architecture. Since the DGSA is intended to address the needs of all DoD organizations, it is a more general statement about the common collection of services and mechanisms any information system might offer and allocates the security services and mechanisms to generic components of information systems.

The DoD organizations that will employ the DGSA have many different missions. The security policy addressed by the DGSA is a general expression of the security requirements commonly found among the mission requirements of DoD organizations. Figure 2-1 shows that security policy and requirements are derived as a result of examining the threats to the mission and are therefore a subset of the mission's requirements. It also indicates the strong relationship among mission, users, information, and policy.

The establishment of security requirements follows the same process whether it is for the DGSA or a specific mission. The process is composed of the following mandatory steps: the information to be managed is identified; the operational requirements for the use of the information are stated; the value of the information is determined; and the potential threats to the information are identified. The security policy for either the generic case (the DGSA) or a specific mission can next be stated in terms of the requirements for:

- Protection for the information based on the potential threats
- Security services that afford the appropriate protection of the information based upon the value of the information and the threats to it

Figure 2-1. Security Policy and Requirements

As stated previously, the DGSA is a security architecture covering the full range of DoD missions and related information system security services and security mechanisms. The development of a mission-specific security architecture, as shown in figure 2-2, begins by applying the DoD security policy to the specific mission requirements to develop a mission-specific security policy, which includes identifying the appropriate security services and mechanisms an information system should offer to satisfy those requirements. The mission-specific information system security architecture is derived from this set of requirements and security services. This mission-specific architecture is stated as the set of mechanisms appropriate for providing the level of protection required. Guidance documents such as the TAFIM, and particularly the DGSA, should be applied to a specific information system architecture to ensure that the necessary security protections are appropriately allocated to specific information system components. Specific security architectures also need to address any applicable policy, public laws, and executive orders. Information system security architects should understand the complete methodology and the way other aspects of the DGSA are taken into account as demonstrated in the examples in section 9.

Figure 2-2. Mission-Specific Security Architecture Development

2.1 DGSA SECURITY POLICY

The DGSA security policy is based on the security requirements cited in the *DoD Information Systems Security Policy* (NSA, 1993), which is summarized as follows:

1. DoD information systems must support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information.

2. DoD information systems must be sufficiently protected to allow distributed information processing (including distributed information system management) among multiple hosts on multiple networks in accordance with open systems architectures.

3. DoD information systems must support information processing among users with different security attributes employing resources with varying degrees of security protection, including users of nonsecure resources if a particular mission so dictates.

4. DoD information systems must be sufficiently protected to allow connectivity via common carrier (public) communications systems.

2.2 DGSA SECURITY REQUIREMENTS

This section describes the DGSA security requirements based on the security policy stated in section 2.1. The four security requirements discussed are Multiple Information Security Policy Support, Open Systems Employment, Appropriate Security Protection, and Common Security Management.

2.2.1 Multiple Information Security Policy Support

Although most current information systems support only one information security policy at a time, there has long been a desire by users to operate simultaneously at multiple sensitivity levels or under multiple security policies (e.g., by using multilevel secure systems) on a single device (e.g., workstation, outboard protocol device). Policy statement 1 above recognizes that support for multiple security policy operation must become more common. The successful implementation of policy statements 1, 3, and 4 largely depends on the ability of information systems to separate users and information at different sensitivity levels or to separate information subject to different security policies. That is, implementations must provide users with confidence that there will not be any security policy violations because shared information systems and communications systems are used that support users operating under differing security policies.

2.2.2 Open Systems Employment

DoD information systems must be open in the sense that potential connectivity among them always is supported, even if a particular request for communication is denied because of a security policy decision. Although the use of open systems as a high-level operational requirement (and the policy statements from which this requirement is derived) may seem to be focused on operational issues, it is equally critical to the DGSA in that it promotes a particular approach to providing information security among cooperating DoD information systems. In the past, isolated systems were created and information was over-classified to satisfy security requirements. Given that users operating under different security policies may need to share components, and that complex policies for sharing and transferring information among users operating under different security policies must be supported, it is critical that truly open systems (both information processing systems and communications systems) be employed. Not only is this requirement directly derived from policy statement 2, but it supports policy statements 3 and 4 as well.

2.2.3 Appropriate Security Protection

Policy statements 2, 3, and 4 refer to information systems being "sufficiently protected" or supporting users by employing varying degrees of security protection. The combination of automated, procedural, and physical methods, from the complete set offered by a particular information system, appropriate for protecting a set of users and information can only be determined by those persons responsible for the particular information and who are able to assess its value and the threats to it. The corresponding generic DGSA requirement is that specific means must be available to users to invoke security mechanisms appropriate to the task at hand.

What constitutes appropriate security protection, in part, is affected by the security protection provided by the communications system that is used among distributed systems. Policy statement 4 requires that when common carrier communications must be used, the information systems must be prepared to provide all of the appropriate security protection. The only service that should be assumed from a common carrier communications system is availability.

2.2.4 Common Security Management

Like the open systems requirement, security management appears to be concerned with operational issues, but it actually provides the foundation for many of the security mechanisms that implement the security services chosen to satisfy the other security requirements. To ensure that distributed information processing is properly supported, the DGSA must address common security management. This commonality will allow security administrators to manage, in a uniform manner, systems that operate under multiple security policies in accordance with policy statements 1 and 2.

2.3 DGSA DERIVED SECURITY REQUIREMENTS

This section first discusses the refinement of the security requirements (section 2.3.1) and then the interaction between mission-related operational objectives and security requirements (section 2.3.2). The process of security requirements derivation is shown by example; it is not intended to identify every possible security requirement. The expectation is that developers will perform similar, but complete, analyses for specific systems.

2.3.1 Security Requirements Refinement

The refinement of the security requirements is stated as a set of security services, functions, or activities that will be allocated among users, administrators (acting on behalf of the users), information systems, and communications systems for a particular distributed information system architecture.

2.3.1.1 Multiple Information Security Policy Support

Several derived requirements are consequences of the need to support multiple information security policies. The most basic of these is the ability to support each security policy independently of other security policies supported in shared information systems or communications systems. Security policy enforcement is dependent on the ability of supporting information systems to maintain reliably the identities of users and the identification of information objects under each security policy. The traditional expression of policy enforcement is that all references by users (or processes representing them) to information objects must be mediated by a reference monitor. The DGSA adopts the reference monitor concept. (Note that any number of reference monitor implementations may be possible.)

When information processing operations are supported by distributed information processing systems, the security policy enforcement for information in transit is commonly supported by mutual authentication, access control, data integrity, data confidentiality, and non-repudiation communications security services. For local (e.g., within a workstation) information processing, a similar set of security services can be applied.

2.3.1.2 Open Systems Employment

When a user seeks to perform functions in a distributed environment, the user must be able to convey information to another user (or a process) that will become the basis for decisions about what (if any) kinds of interaction will be allowed. The DGSA presumes that international standard protocols (or at least national or DoD standards, not industry proprietary schemes), information, and mechanisms will enable users to determine the capabilities and environment of other users or system processes with which they attempt to communicate. The determination may be made on the basis of information available before any communication is attempted (e.g., from a directory service), or where the determination is made as part of the initial communications service negotiation, or a combination. The result of such a determination might be that (within the information security policies shared by the users) the only common capability is to share only non-sensitive information or that no further communication is possible.

Beyond the normal means to begin distributed processing, standards for the representation and exchange of security information are needed. Some of this information is made available as part of the communications exchanges and some is provided through security management-related exchanges. Taken together, this information is used in the provision of various security services.

2.3.1.3 Appropriate Security Protection

The requirement for appropriate information systems security protection dictates that security mechanisms must be identified that implement security services at the level of protection required in security policies. Since some security mechanisms may be used to provide (parts of) multiple security services and some security services may be implemented by multiple mechanisms, a determination must be made that the mechanisms are appropriate individually and in combination. Initially, this is a technical activity, but the final determination involves deciding whether shortfalls in the collected security mechanisms can be accepted or whether additional measures must be put in place. This determination must be made by the users of mission information, or as is most common, the accreditor who represents the users.

2.3.1.4 Common Security Management

The basic elements that must be managed within the DGSA are users, security polices, information, information processing systems that support one or more security policies, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. For each of these elements, the managed objects that constitute them must be identified and maintained. For example, users must be known and registered, the security policies must be represented and maintained, and information objects must be identified and maintained. The format for presenting the information in managed objects and operations on them must be standardized. Section 6 presents a detailed discussion of these managed objects and an architecture for security management within the DGSA.

2.3.1.5 Summary of Security Requirements Refinements

The requirements refinements discussed above are summarized in table 2-1.

2.3.2 Interaction Between Mission-Related Operational Objectives and Security Requirements

This section describes the interaction between mission-related operational objectives and security requirements. This presentation is designed to promote a thought or investigative process that should be applied to specific missions. Not all of the operational objectives discussed here pertain to every mission.

2.3.2.1 Prevalence of Enterprise Initiatives

DoD-wide enterprise initiatives, such as Center for Information Management (CIM) and C4IFTW, impose operational objectives that have an impact on security. CIM promotes information centralization, information access, and interoperability. All three of these activities eliminate the idea of isolated or stand-alone implementations as a means of providing security. Their effect on security requirements is the need to consider both the coexistence of varying sensitivities of information on the same information system and the provision of proper separation, authentication, labeling, and access control. C4IFTW is designed to provide the war-fighting soldier with access to any information needed to do the job, regardless of sensitivity, media, or branch of Service. Such operational objectives also provide security challenges and considerations. System interfaces are quite different for war-fighting equipment, thus presenting new authentication issues. Access to the information in a pull-from (information-on-demand) mode emphasizes both interoperability and availability requirements. The integration of voice, imagery, and data requires data correlation and a general secure display (windows) implementation. The implications of CIM and C4IFTW and any other relevant initiatives should be considered for their effects on specific missions.

Table 2-1. Summary of Security Requirements Refinements

Multiple Security Policy Support	**Open Systems Employment**	**Appropriate Protection**	**Common Security Management**
– Enforce security policy – Maintain user identities – Maintain information identification – Provide data integrity service – Provide data confidentiality service – Provide non-repudiation service	– Provide common security capability identification – Use standard security information exchanges – Use standard security information representations – Provide authentication service – Provide access control service – Provide availability service	– Identify appropriate security mechanisms that provide required level of protection for each security service (individually and in combination)	– Identify and maintain user information managed objects – Identify and maintain information system managed objects – Identify and maintain supporting security function managed objects – Use standard managed object representations

2.3.2.2 Use of Off-The-Shelf Equipment

Economics have always been a driver in decisions to employ security solutions for information systems. Implementation of automated security measures has raised systems costs with questionable returns on investment. One of the reasons that costs of security measures have remained high compared to their value is that security measures have been implemented in specialized, often retrofitted, components. Particularly in the face of current budgetary constraints, it is highly desirable that security features become standard elements of commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) equipment so that security has minimal impact on price. For this to happen, vendors must be persuaded to create products with security features that are integral parts of those products. Vendors will need to be convinced that a real market for such products exists. Evaluation, certification, and accreditation must become streamlined and conclusive processes so that the vendors can be assured of reasonable investment and return. Creation of a viable security product market will depend on use of standards for commercial, international, and DoD use. Availability of COTS and GOTS products with integral security features will affect the ability to achieve mission security requirements.

2.3.2.3 Need for Increased Connectivity

A common and significant operational objective is to take advantage of computer and communications technology to accomplish the mission at hand. This objective can be partially achieved by increasing the potential for connectivity, making additional resources available. Other operational objectives demand that such increased connectivity cannot increase cost significantly. One approach to increased connectivity is to employ commercially available, common carrier networks. However, this approach introduces significant potential risks. There is always the possibility that a hostile entity, with access to the network, will use any means affordable to mount attacks on information systems using the network. The resulting security requirement is that the security mechanisms chosen to protect information must be adequate to deter such a hostile entity.

Increased connectivity and use of common carrier systems present a perfect environment for DoD-wide interoperability. The connectivity to common carriers will dictate lower layer (International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Reference Model (RM), ISO 7498 (ISO, 1984) Layer 3 and below) standard protocols, while the DoD missions will have to address upper layer (ISO Layer 4 and above) standards for interoperability between local environments. This standardization will include authentication information, security protocols, key management and distribution, and security management information. Equivalent standards use for voice communications should be used. Additionally, the potential threat of a hostile entity will require standard methods of evaluating the protections afforded to information and other resources to assure that remote user environments are providing equivalent protection.

2.3.2.4 Access to Information and Resource

A common operational objective is to provide users with access to any information and resources needed to complete a task. This objective includes operational concepts such as information pull, distributed processing, and information sharing. Some missions will require support by non-DoD personnel and resources.

Security considerations cause enclaves to arise based on mission criteria that require separation of users and information, while operational objectives create the need to traverse enclave boundaries. For example, pull-from may mean information will come from another enclave. This requires interoperability of communications and security services. In dealing with access to and sharing of information and resources, the following security implications must be considered: establishment and separation of enclaves, interpretation and exchange of information in standard forms, and management of information.

Transparency in distributed processing is an often stated objective, that is, users wish to behave as if all resources are locally available. Users wish to be able to be authenticated once to the local system and then transparently interact with the other systems to access resources. The effect of this objective on security is that information systems must have adequate local authentication schemes and security management mechanisms that free the user from the burdens of procedures such as multiple logins.

2.3.2.5 Certification and Accreditation

Certification is the process of determining the effectiveness of all security mechanisms. *Accreditation* is the process by which an organization (or an individual on behalf of the organization) accepts or rejects operational responsibility for an information system’s performance, including security, in supporting their enclaves.

Certification and accreditation are complementary procedures that need to be consistent, uniform, and applicable across DoD systems and products. Certification procedures have lacked uniformity and a clear path to completion. This deficiency has caused tremendous frustration on the part of both users and developers of systems. In many cases, accreditation procedures are subjective and ad hoc. The results of these procedures applied to particular products and systems should be of value to evaluators and accreditors of products and systems that have common elements. The challenge is to develop a set of uniform procedures that will limit and reduce the time to achieve product and system acceptance and that will eliminate disparities in the accreditation process. Uniform procedures will ensure consistent and interoperable security support for an enclave throughout a distributed environment.

Certain specific information is needed in the certification and accreditation processes that generally is not available today. Knowing the effectiveness of security mechanisms is an important part of determining how well required security services are supported. Knowing how a collection of security mechanisms interact and support one another is important in assessing whether mission requirements have been met while minimizing security risks.

2.3.2.6 Need for Separation

Most missions will require the creation of several groups or enclaves joined together to achieve some specific purpose. It is also likely that the individuals involved will be members of more than one of these enclaves and will need to operate in two or more simultaneously. Organizations can no longer afford to build separate systems to support each of these enclaves, nor is it effective to require the user to change interface components (such as a workstation) every time the need arises to operate in a different enclave. The resulting security requirement is the establishment of criteria for mechanisms that allow multiple enclaves to share systems and information while guaranteeing the separation of information and users as necessary.

2.3.2.7 Maximizing Return on Investment

Operations today must exist in an environment in which major trends tend to be at odds with one another. Technology advancement has provided an opportunity to create an operational vision barely imaginable a few years ago. However, the high cost of transitions and diminishing budgets act against employing the new technologies. Intelligent strategies which may not reduce up-front costs but show valuable long-term benefits and reductions in costs will win favor. These strategies must support the long-term operational objectives. Such strategies include portability of applications and other software, continuous upgrades of hardware and software, ensuring scalability of applications and communications resources, reuse of software components, and reuse of certification and accreditation results. Each strategy has the post-transition value of providing low-cost growth paths if supported properly. Each strategy has an effect on security. Recertification of systems and products after change may be the most important of the strategies in its long-term payoff.