# SECURITY POLICY

## TARGET, CONTENT, & LINKS

### WHITE PAPER

**Frank T. Bass**

**8 June 1998**

**τΩ Engineering, Incorporated**
**423 Seminole Drive**
**Montgomery, Alabama 36117**

## Executive Summary

The purpose of this paper is to propose a standard security policy template with the following characteristics.

- Policy target is toward senior-level managers for the expressed purpose of gaining their support for an enterprise-wide security program. Details are left out so the appeal to this readership is stronger.

- Policy content includes high-level security requirements, policy descriptions, a security concept of operation, and an allocation of security features to system architecture elements to show which "pieces" of your system enforce which policies.

- Policies implementations occurs (e.g., *detailed* policy statements) in an End User Manual (or like content in a Security Features User's Guide) and a System Administrator's Manual (or like content in a Trusted Facility Manual).

In addition, there is a description of how the security policies link to other program actions such as criticality and sensitivity assessments, development of security specifications, security enforcement modeling, security test and evaluation, and the like.

# Security Policy: Target, Content, & Links

## Introduction.

*Webster* defines policy as "A definite course of action adopted for the sake of expediency, facility, or the like."

So, what about definite courses of action to protect sensitive data? In today's IT environment, there seems to be a very large number of organizations paying nothing but lip service to developing policies reflecting enterprise security. A recent article, appearing in *SC Info Security News Magazine*, November 1997, titled *Senior Executives' Attitudes to Computer Security*, indicates: "There is much evidence, both statistical and anecdotal, that many senior managers are not taking the issue of security seriously. For instance an *Information Week* survey of 1,271 computer managers found that only 22 per cent believed their senior managers thought information security was 'extremely important'." In that same article there is further evidence— "Earlier this year, Kasten Chase, the security networking company carried out a survey of police forces that concluded that only 25 percent of police forces were currently formulating an IT security policy." This survey result reflects findings in many other segments of U.S. business, Government, and industry.

This lack of attention toward security and the dearth of strong security policies results in an absence of the foundation necessary for protecting valuable resources. It would seem then, we need more emphasis on security policy development not only because there is a requirement to protect data, but also because there may be a lack of focus on the part of responsible managers to direct that data protection.

The purpose of this paper is twofold. First, you need to target strong security policies toward a readership consisting of senior-level managers, because it is this readership that makes enterprise-wide business decisions. Thus, you need their support to implement robust information protection schemes and procedures.

Secondly, you need a security policy content that establishes a foundation for all subsequent security-related system and organizational actions.

To accomplish this purpose, we'll look at (1) targeting policies toward those who make enterprise-wide business decisions, (2) what makes strong policy content, (3) how you implement policy details, and finally (4) how your security policies form links to other security and system development activities.

For the purposes of this paper, keep in mind security policies must be high-level courses of action. This high-level attention is necessary to appeal to our target readership. Details should be left to policy implementation. Focus on the "Policy" as the foundation for all subsequent security directions within the enterprise and as an integral part of the overall system development methodology—not something you "bolt" on as an afterthought.

## Policy Target.

For policy effectiveness, you need to decide upon your target audience—**before** you begin. Therefore, in keeping with our premise of senior-level involvement, we want to target our "Policy" toward those who make business decisions in the enterprise. The "Policy" should be an opportunity for senior managers to "sign up" to an organizational (or enterprise-wide) security program.

To accomplish this targeting, you must ensure the "Policy" document relates to your organization from a high-level perspective. No senior-level manager is going to "wade through" a document containing security-ese, unfathomable technical jargon, and endless detail. So, if your purpose is senior-level backing for organizational security, you've got to eliminate the details and focus on—you guessed it—POLICY.

I guess the question might arise in some circles as to the merits of senior-level involvement in anything. After all, isn't it senior management's plight to go around mucking up enterprise activities? Isn't "real" work the purview of those in the trenches? Actually, the answer to both of these questions is no. If you want emphasis on a subject (i.e., monetary involvement and sustained support), you must convince those who make financial AND technical judgments that it makes business sense to protect valuable enterprise resources.

What you need is to gain the support of those who make final business decisions in your organization. To do that, you focus the "Policy" on a "course of action" supporting enterprise-wide protection of your critical assets from an "overview" perspective.

## Policy Contents.

Previously, I mentioned our target audience and suggested that "Policy" content be kept at a very high level to avoid possible disinterest on the part of senior management. Now, let's focus on the details of "Policy" content to see what goes in there, and how the content will match our requirements for keeping everything at a high level.

Before we do that, however, we need to establish a focus around which "Policy" content will revolve. So, let us propose a pivotal theme whereby "Policy" is central for developing and maintaining secure computer and network systems. It will map courses of action for system developers, provide first-level security requirements for traceability to those requirements, and will interface with the system's security architecture. In this manner, we demand our "Policy" be integral to the overall system's foundation so security becomes "woven" into its "fabric" and does not become a "bolted-on" course of action.

We now have our target readership and our focus. I'm going to propose our "Policy" contains the following four categories of information.

- High-level security requirements.
- Policy descriptions based on requirements.
- Security concept of operation.
- Allocation of security enforcement to architecture elements.

**High-level Security Requirements.**

The high-level security requirements are statements describing the features you want in your system to enforce your security policies. This section is broken into four types of requirements:

- *Discipline Security Requirements*: Discipline security requirements include communications security, computer security, operations security, emanations security, network security, personnel security, information security, and physical security.
- *Safeguard Security Requirements*: Safeguard security requirements consist of access control, archive, audit, authenticity, availability, confidentiality, cryptography, identification and authentication, integrity, interfaces, markings, non-repudiation, object reuse, recovery, and virus protection.
- *Procedural Security Requirements*: Procedural security requirements incorporate access policies, accountability, continuity of operations, and documentation.
- *Assurance Security Requirements*: Assurance security requirements include certification and accreditation packages and "sustaining" planning documents.

See Appendix A, High-level Security Requirements, for an example set of security requirements. Note: This set is not inclusive of every type of requirement.

**Policy Descriptions.**

This portion of our security policy prescribes and adopts an architectural perspective for security measures required to fully trust component systems to meet functional mission requirements and security mandates at an acceptable level of risk.

The security policy and its architecture specify a cohesive protection strategy to satisfy the following objectives:

- Operate safely and securely at an acceptable risk level.
- Control information and resource sharing essential to meet operational requirements for integrated support capabilities.
- Conduct structured Security Test and Evaluation (ST&E) activities essential to ensure implemented security mechanisms function as designed and intended.
- Perform high confidence risk assessment in conjunction with certification.
- Field component systems upon cognizant accreditation authority rendering an informed deployment decision to operate them in the security mode and sensitivity level required by the operational environment.

Figure 1 portrays a high-level overview of the security architecture. Some key points about its strategies and concepts follow.

a. Strategies. The left side of the diagram shows the strategies verifying each level of the security architecture.

    1. *Risk Assessment*. The Risk Assessment strategy identifies threats, vulnerabilities, and risks. The Risk Assessment thus defines which Disciplines, Safeguards, Procedures, and Assurances apply and must be used to mitigate against the associated risks.

    2. *Security Test and Evaluation*. Next, the Security Test and Evaluation confidence verifies the Safeguards and Procedures adequately and appropriately protect the information component systems handle.

    3. *Certification*. Certification provides the "convincing evidence" the protective security measures are technically adequate and meet the security policy being pursued.

    4. *Accreditation*. Accreditation affirms the associated risks are acceptable and authorizes mission use.

b. Concepts. The right side of the diagram shows the security architecture's concepts and their elements. Each concept has an associated strategy as described above.

    1. *Disciplines*. Disciplines set forth fundamental security principles in that they encompass the laws, regulations, rules, and practices necessary to properly protect component systems and the sensitive information you entrust to them.

    2. *Safeguards*. Derived from the several Disciplines, Safeguards constitute essential functions, features, and mechanisms that enforce rules about protecting sensitive information whether it is in transit on a communications link, stored in a computer, or manipulated by a functional user at his or her terminal.

3. *Procedures*. Next, Procedures deal with the steps necessary to properly configure and maintain the Safeguards. In some instances, procedures themselves are safeguards (e.g., checking an access roster to affirm who may enter a sensitive facility without an escort).

4. *Assurances*. Lastly, Assurances address the "proof" and "approval" that the security measures are in place, operate as intended, and do so at an acceptable level of risk. Equally important are the sustaining plans essential to maintain a secure posture in a life-cycle environment (i.e., Contingency Plan, Security Training Plan, Certification and Accreditation Plan, and the like).

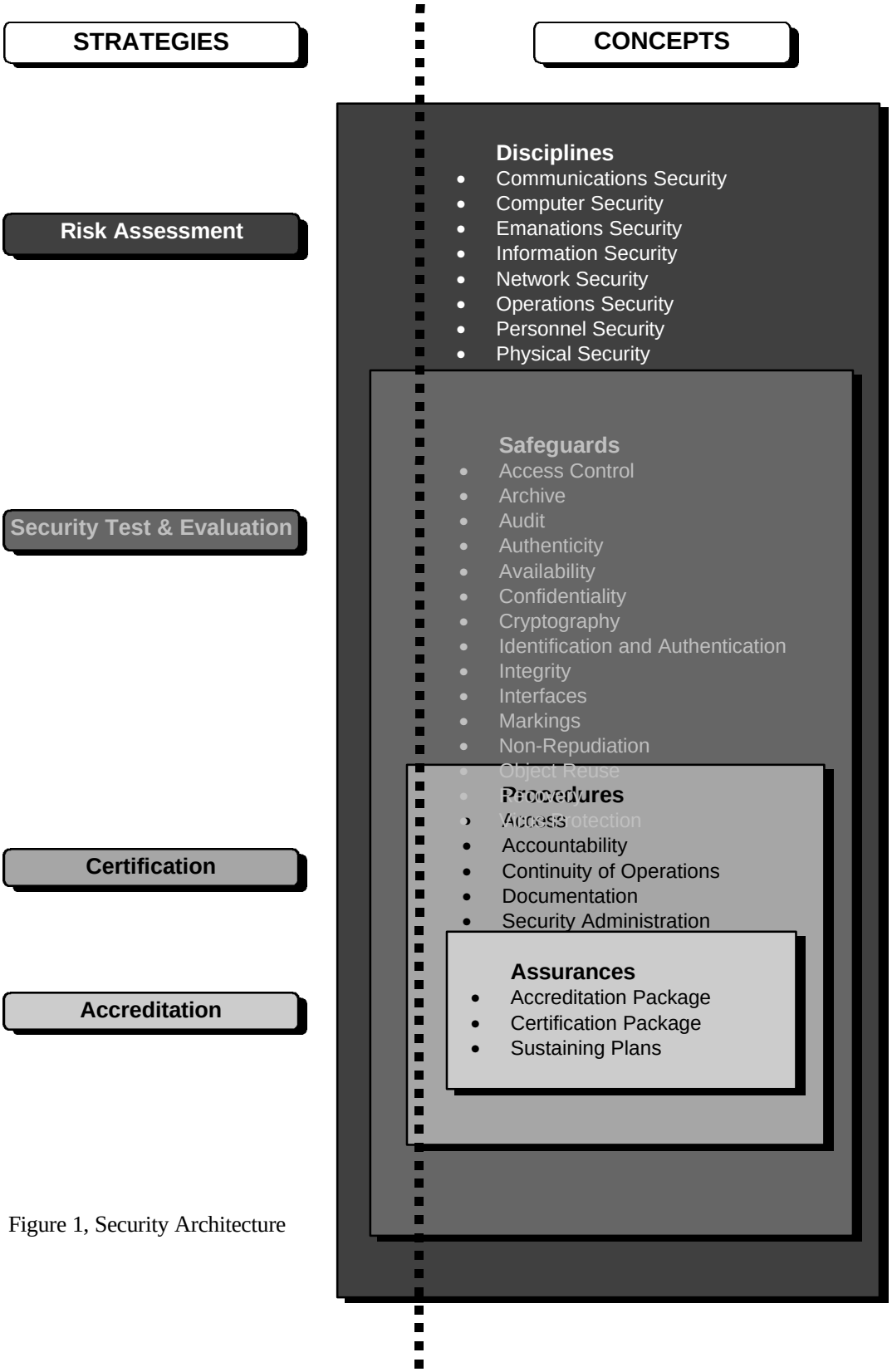


Figure 1, Security Architecture

The policy descriptions focus on security disciplines, safeguards, procedures, continuity of operations, and documentation. Each subset of this portion of the policy describes how the system's architecture elements will enforce security. See Appendix B, Policy Descriptions, for an example of these descriptions.

**Concept of Operations.**

This section provides a concept of operations outlining the basic roles, responsibilities, functions, and overall mission and technical implementation of the System Program and its infrastructure. The infrastructure components are application systems under oversight of organizational functional components.

The Security CONOPS focuses on:

- Mission.
- Communications.
- Encryption.
- Operational Security Considerations.
- Facility, Personnel, and Maintenance Rules.
- User Interface Rules.
- Idle Time Management.
- Privately-owned, Public Domain, and Shareware Software Rules.
- Continuity of Operations Planning.
- Fraud, Waste, and Abuse.
- Training and Awareness.
- Virus Protection Policy

See Appendix C for an example of a security concept of operations.

**Architecture Element Allocation.**

This section establishes a computer security architecture allocation to each major computer system element of the Program. This provides an overview of each architecture element and the security feature(s) it provides.

Data in this section is in a tabular format and covers:

- Component system architecture elements that implement your security requirements.
- Mapping rationale for allocating security requirements to system architecture elements. And,
- Mapping summary data showing security requirements allocated to component system elements.

This tabular format allows senior management to readily visualize what architecture elements will enforce the various security features. See Appendix D for example tables showing these allocations.

## Policy Implementations.

The information about security policies we covered above focused on high-level aspects of policy targeted toward senior-level management. You'll recall our purpose was to produce a product which senior managers would use to "sign on" to an enterprise-wide security program. This previous segment ends the discussion of the actual Security Policy document and its content. However, there must be a way to produce detailed information for implementing those policies. We do this with two products—an End-user Manual (like content—Security Features User's Guide-SFUG) and a System Administrator's Manual (like content—Trusted Facility Manual-TFM).

**End-user Manual or SFUG.**

The purpose of the End User Manual or System Security Features User's Guide is to address Trusted Computing Base (System Trusted Element) protection mechanisms, functions, and features that pertain to the operational functional users and their interfaces with component systems. That is, this Guide is for people who access the system via workstations.

The SFUG has two parts—the first part gives background information about the system, provides an overview of its security measures, highlights the assumptions and constraints which apply, and defines *terms-of-art* for concepts or phrases in the Guide. The second part contains information necessary to perform official duty tasks consistent with the System Security Policy. Note, this Guide provides essential security information—it does not overly duplicate information in other publications.

The Guide serves several roles for functional users who access your system via their workstations:

a. It is the overall Security Features User's Guide (SFUG) for your system.

    1. It provides authoritative instructions for mission-oriented *Functional Area Supervisors* and their associated "community-of-interest" (*Functional Users* who employ system functions, features, and capabilities to perform their official duty mission tasks).

    2. It complies with guidance in policy and other security regulations and directives for "user documentation" necessary to properly employ protective countermeasures and safeguards.

b. It cross-references other Security Features User's Guide information. Note: You place applicable security publications associated with products such as operating systems and database packages here.

c. It also cross-references other important security-related information. Note: You place applicable system-related security documentation references here.

Using this Guide, you can meet your obligations to protect your system against:

a. Confidentiality Loss (e.g., prohibit "compromising" classified or other sensitive data).

b. Data Integrity Loss (e.g., prohibit "unauthorized" destruction, loss, use, or access).

c. Service Denial Hazards (e.g., inhibit "malicious acts" or other conditions which deny authorized use or access to the system needed to meet operational mission requirements).

The scope of this document is:

a. It recaps System Security Policy statements in the Descriptive Top Level Specification (DTLS);

b. It highlights security countermeasures that provide the encompassing environment—such as Physical Security—in which System components and user *community-of-interest* members function and perform official duty tasks;

c. It sketches security safeguards the system itself uses to identity, separate, and control its protected resources (e.g., a program or file)—Computer Security;

d. It provides authoritative instructions for mission-oriented users who employ system functions, features, and capabilities to perform their official duty mission tasks whether they are a *Functional Area Supervisor* or an associated "community-of-interest" member. And,

e. It cross-references other Security Features User's Guide information (see *Security Features User's Guide cross-references*):

General content for this document includes:

- System threats.
- Externally enforced countermeasures.
- Internally enforced safeguards.
- Security operating mode(s).
- Assumptions and constraints.
- System trusted element protection mechanisms.
- System trusted element protection mechanism descriptions.
- Trusted official and functional user relationships.
- Security-related advisories and responses.
- Cross references to other documents.
- Operating security mode guidelines.
- Data aggregation rules.
- Appendices covering definitions, a desktop guide, and a quick security card.

The details in this policy implementation document cover instructions for interacting with the security environment, procedures for securing information, and responses to security actions.

**System Administrator's Manual or TFM.**

The System Administrator's Manual or Trusted Facility Manual (TFM) addresses the controlled functions and privileges when running a secure facility. This Manual further provides Trusted Officials such as System Security Officers, System Administrators, and/or System Operators) with:

a. Basic security information about a secure system;

b. A synopsis of individual system component documents (i.e., component Trusted Facility Manuals, administrator guidance, and the like) that System Trusted Officials must use, and;

c. Specific set up and day-to-day secure system operational guidance.

This document provides system-specific guidance and instructions to Trusted Officials and integrates appropriate information from existing TFM and TFM-like content in other system documentation. Included are tips for finding information in those commercial publications, actions required to support system applications software, and precautions regarding set up and day-to-day secure operation.

The TFM is broken into:

a. Section 1 of the Manual provides document scope and assumptions and constraints, and defines important terms Trusted Officials must know or be familiar with.

b. Section 2 describes the System hardware, software, and network configuration, summarizes security protection mechanisms available with the System component systems. It further describes:

    1. The System Security Policy;

    2. How the system achieves its security accountability goals and assigns Trusted Official responsibilities for helping to meet those goals;

    3. How the system achieves its security assurance requirements and what Trusted Officials must do, both upon initial set-up, and on a recurring basis to maintain sufficient assurance the System Security Policy will always be faithfully enforced. And,

    4. Appendices listing acronyms used, a bibliography, mandatory parameter settings for a secure system, and a summary of system component security mechanisms.

This Manual serves several roles for Trusted Officials who are responsible for establishing and maintaining a secure system operation:

a. It is the overall Trusted Facility Manual (TFM) for your system.

    1. It introduces System Trusted Officials to the basic concepts essential to set up and operate a secure system.

    2. It presents the system security protection strategy and lists the vendor-provided documents Trusted Officials (System Administrators, System Security Officers, and System Operators) will need. It goes on to explain their purpose, interrelationships, and how each satisfies system security and mission requirements.

    3. It provides system-specific requirements and procedures to set up functional user accounts, determine authorized user and process permissions, implement mechanisms for protected resources, and manage security enforcement mechanisms implemented on the several component systems that together supply the system mission applications support platforms.

    4. It cites precautions—specific information and warnings—that help prevent unwanted and potentially very serious consequences resulting from unwitting or errant configuration actions.

b. It cross-references other Trusted Facility Manual information.

c. It also cross-references other important security-related information:

    1. System Security Features User's Guide.

    2. [Vendor-supplied trusted operating system TFMs].

3. [Workstation operating system TFMs].

Using this Manual will help you meet your obligations to protect your system against:

a. Confidentiality Loss (e.g., prohibit “compromising” classified or other sensitive data).

b. Data Integrity Loss (e.g., prohibit “unauthorized” destruction, loss, use, or access).

c. Service Denial Hazards (e.g., inhibit “malicious acts” or other conditions which deny authorized use or access to the system needed to meet operational mission requirements).

General content of the TFM includes:

- Assumptions and constraints.
- System security policy synopsis.
- Accountability.
- Assurances.
- Appendices covering terms, trusted facility operations, component security mechanisms summary, and security publications cross references.

Overall, the TFM provides:

- Configuration instructions for operating systems and applications.
- Handling directives for data.
- Operational directives.
- Installation instructions.
- Configuration management of software components.
- Physical security practices and procedures.
- Software distribution instructions.

## Policy Links.

Our last topic on security policy deals with how the policies link with other system development actions. Some of these actions are input to the policy and some are a result of defining the policies.

*Sensitivity, criticality, vulnerability*. Before you can define any policy elements, you must analyze the data and information the system will process, store, and/or transmit. You cannot understand policy outside the parameters of data sensitivity or criticality. If your data is very sensitive, then your policy will consist of enforcement parameters consistent with the sensitivities involved. If the information within the boundaries of your system is critical to your organization's survival, then you must implement protection schemes necessary to keep out unauthorized users and prevent unauthorized modifications to that information.

Just as important as understanding the nature of your data, you must assess your system for vulnerabilities. If you know where your system is vulnerable, you can develop policies which direct the implementation of security features to reduce the risks associated with the known vulnerabilities.

*Business processes - manual and automated processes should follow policies*. Once you developed your policies, is would seem reasonable to expect you would tailor and/or design your business processes to support those security policies. It would not promote a stable security environment if you routinely followed business practices that violated your protection schemes.

*Security architecture - element choice for enforcing security*. If you have strong security policies and you design your business processes to execute your policies, then it seems logical to put in place a set of system architecture elements supporting both. Each system component must assist (as much as possible) in reducing the risks associated with the vulnerabilities you discovered during the early stages of development. Thus, your system's architecture is a direct result of the security policies you refined earlier.

*Security models - provides the direction security models will take*. When requirements dictate you model your system's enforcement mechanisms, you use security policies to direct the design of your models. You take the high-level requirements in the policy document and model each security discipline (access control, audit, identification and authentication, and the like). The model will illustrate how each discipline attempts to enforce your system's policies.

*Security requirements and specifications - detailed requirements and specifications directly traceable to the high-level policy requirements*. The next logical step in implementing policies is preparation of detailed security requirements or specifications. For example, if your policies support distinguishing between data sensitivity levels, then its possible you may need some form of labeling and data marking functions. If your applications use a windowing environment, it may be necessary for your designers to color code window banners and associate specific colors with sensitivity levels—red for the highest classification, blue for the next highest, and so on. In other words, your detailed security specifications implement the high-level policies you advanced previously.

*Software Design - design includes hard-coded policy implementations*. Your software design will directly reflect your security policies because of the specification step we just mentioned. Each specification requires a code module or modules to implement it. Applications, including databases, embody code to implement each high-level security requirement and resulting specification(s).

*Test procedures - ensures all requirements get tested*. When you complete software design, you will enter the testing phase of development. To ensure you thoroughly test all security requirements, you

match all of the detailed specifications to test procedures. You can accomplish this by designing a test matrix showing each specification matched to one or more test procedures.

As you can see, not only do your policies provide a foundation of all system security actions, they also contribute to a complete system-wide security requirements traceability web linking every policy to every requirement.

## Summary.

I set out in this paper to propose a security policy with the following characteristics.

- A policy targeted toward senior-level managers for the expressed purpose of gaining their support for an enterprise-wide security program. Details are left out so the appeal to this readership would be stronger.

- "Policy" content includes high-level security requirements, policy descriptions, a security concept of operation, and an allocation of security features to system architecture elements to show which "pieces" of your system enforce which policies.

- Detailed policy statements are in an End User Manual (also known as an SFUG) and a System Administrator's Manual (or TFM).

In addition, I described how the security policies linked to other program actions such as criticality and sensitivity assessments, development of security specifications, security enforcement modeling, security test and evaluation, and the like.

The bottom line is this—security policy is the focal point for many of the actions you will take during design, development, implementation, and maintenance of your system. Without strong security policies, you will not have a sound foundation upon which to develop and/or maintain your system. Without strong security policy, you will not be able to say, with strong conviction, you have a system that protects your organization's sensitive and/or critical information.

# Appendix A High-level Security Requirements

This appendix contains an example set of high-level security requirements. The information does not imply completeness. Your system may have other high-level requirements that apply. Note: Everywhere you see information in brackets ([ ]), you replace it with your own system's data.

**Discipline Security Requirements (DSR)**.

*Communications Security - DSR01*. [SYSTEM] component systems must comply with COMSEC requirements in: [place relevant documentation references here].

*Computer Security - DSR02*. [SYSTEM] component systems shall achieve [system security level objective such as Controlled Access Protection] functionality and therefore must comply with COMPUSEC requirements in: [place relevant documentation references here].

*Emanations Security - DSR03*. [SYSTEM] component systems must comply with EMSEC guidance in: [place relevant documentation references here].

*Information Security - DSR04*. Policies in [place relevant documentation reference(s) here], apply to [SYSTEM] component systems.

*Network Security - DSR05*. Security-related protocols [SYSTEM] component systems use must be shown to be consistent with: [place relevant documentation references here].

*Operations Security - DSR06*. [Place relevant documentation references here], guidance applies to [SYSTEM] component systems with regard to operations security.

*Personnel Security - DSR07*. Personnel security rules in [place relevant documentation references here], apply to [SYSTEM] component systems.

*Physical Security - DSR08*. Physical security rules in [place relevant documentation references here], apply to [SYSTEM] component systems.

**Safeguard Security Requirements (SSR)**.

*Access Control - SSR01*. Access Control features shall define and control access between named users (e.g., humans and processes) and named objects (e.g., files and programs). [SYSTEM] component systems shall provide Discretionary Access Control (DAC) functions to restrict access to object(s) (files, records, programs) based on the identity of the subject(s) (person or process) and need-to-know, need-to-use, or need-to-invoke privileges. Note: You may also have a need for Mandatory Access Control in which case you will need an additional security requirements to cover MAC.

*Security Profile Tables - SSR02*. [SYSTEM] component systems shall maintain and protect, from unauthorized access or modification, one or more security profile tables (or equivalent) containing: identification and authentication data, DAC rule enforcement representations (logic tables), data set to object permission mapping vectors, and, similar data the system uses to logically associate the security policy with its enforcement mechanisms or algorithms.

*Archive - SSR03*. The system shall provide archival features and associated records to permit mission data reconciliation during system recovery activities (e.g., recover partially processed messages) and to adjudicate non-repudiation disputes arising from message exchanges (e.g., affirm receipt of disputed

messages). Additionally, you shall enable short-term archives (sometimes termed “roll back” logs) to ensure transitory information is available after a failure.

*Audit - SSR04*. [SYSTEM] component systems shall create, maintain, and protect from modification and unauthorized access or destruction, a security audit trail of [SYSTEM] auditable events (e.g., user logon, logoff; file open or close, and the like). The System Administrator shall have capabilities to selective invoke security audit trail recording options.

*Authenticity - SSR05*. Cryptographically-based Message Digest Functions or other computationally strong mechanisms shall ensure there is an exact character-for-character correspondence between message content as originated and the message as received. Whether affirmative or negative, the system shall record results from authenticity checking algorithms in the security audit trail.

*Availability - SSR06*. [SYSTEM] component systems shall incorporate features and capabilities to sustain a system availability sufficient for responding to queries about messages within (n) hours.(e.g., uninterruptible power supplies, alternate communications paths). Other availability enhancing features are: transaction format validation, protected or un-modifiable entry fields, edit checks for allowable data ranges, and the like.

*Confidentiality - SSR07*. [SYSTEM] component systems shall incorporate explicit confidentiality mechanisms to protect against unauthorized disclosure or information access by, for example, granting explicit access privileges and access modes according to a user’s official duty assignment tasks. Confidentiality enforcing mechanisms shall permit selective enforcement on an individual entity basis (e.g., a single named person or file). The system shall record results from algorithms which adjudicate confidentiality rules in the security audit trail. Consistent with confidentiality rules, object reuse features must purge residual information when storage media will be reused.

*Cryptography*.

- Cryptography Devices - SSR08. [SYSTEM] component systems shall protect [SYSTEM] information using cryptographic devices against unauthorized disclosure prior to transmission over vulnerable media (e.g., circuits connecting a site to communications switching nodes). The system shall also support specialized cryptographic devices implementing non-repudiation mechanisms.

- Key Management System - SSR09. [SYSTEM] component systems shall provide a cryptographic key management infrastructure supporting all cryptographic devices in [SYSTEM] component systems.

*Identification and Authentication - SSR10*. [SYSTEM] component system identification and authentication features shall demand all users explicitly identify and authenticate themselves before performing any further action the component system will mediate. For example, the SA shall register all users with the component systems via user_IDs appropriate for the purpose (e.g., ASCII character strings for humans, binary sequences for electronic systems). Passwords shall be sufficiently "strong" to resist trivial attacks via password guessing techniques (see also *User Interface Rules*, for additional details about user_IDs and passwords). Except for necessary user_ID [account] registration and subsequent maintenance actions by System Administrators, the system shall protect all identification and authentication features and associated parameters from unauthorized modification or access. Note: The System Administrator shall not grant access to [SYSTEM] component systems by "default user_IDs" other than those necessary for initial program load or applications release install actions; the SA shall disable all other "default" accounts by purging them.

*Integrity*.

- Information Integrity - SSR11. [SYSTEM] component systems shall provide information integrity functions to safeguard against tampering or unauthorized data changes. Information integrity features shall also safeguard against computer viruses or other malicious software entities.

- System Integrity - SSR12. [SYSTEM] component systems shall provide hardware and/or software features to periodically validate the correct operation of applicable security features within on-site hardware and firmware elements, if any. In addition, appropriate mechanisms must protect hardware, software applications, and data from direct or inadvertent tampering (e.g., unconditionally forbid access to system files and programs—except for essential configuration actions by the System Administrator).

*Interfaces*.

- External Interfaces - SSR13. Explicit, ***never implicit***, access control privileges and access mode parameters shall impose and enforce confinement rules to safeguard against unauthorized access to individually or mutually protected resources or capabilities potentially or actually made available via external interfaces. The system shall record permitted [forbidden] resource or capability sharing event outcome decisions in the security audit trail.

- Internal Interfaces - SSR14. Explicit or implicit access control privileges and access mode parameters shall impose and enforce confinement rules to safeguard against unauthorized access to individually or mutually protected resources or capabilities potentially or actually made available via internal interfaces. The system shall record permitted [forbidden] resource or capability sharing event outcome decisions in the security audit trail.

*Markings - SSR15*. [SYSTEM] component systems shall, as appropriate, mark output products (e.g., paged, hardcopy output) with a warning banner and trailer page banner consistent with the [appropriate security operating mode] rules. For example, the banners should indicate the most sensitive information authorized for the specific component system—[appropriate security classification or organizational security-level designation]. In like manner, display devices shall also incorporate appropriate marking features for information made available for human viewing.

*Non-Repudiation.* [SYSTEM] component systems shall provide mechanisms to support non-repudiation rule enforcement.

- Non-Repudiation of Origin - SSR16. [SYSTEM] component systems shall incorporate a digital signature mechanism for verifying a claimed originator.* The mechanism shall provide strong digital evidence of the binding between the identity of a party originating a message and the exact contents of the message.

- Non-Repudiation of Receipt - SSR17. [SYSTEM] component systems shall incorporate a digital signature mechanism for verifying a claimed recipient.* The mechanism shall provide strong digital evidence of the binding between the identity of a party receiving a message and the exact contents of the message.

- Trusted Time Stamp - SSR18. [SYSTEM] component systems shall incorporate a strong digital mechanism for verifying a claimed time stamp.* The mechanisms shall provide strong digital evidence of the binding of the time-of-event of a message to the exact (character-by-character) contents of a message. The event could be origination, passage through a notarization server, or receipt by the final recipient.

| |
|---|
| **Any alteration, deletion, addition, or misrepresentation shall be detectable and provable to an impartial third party. Thus, you cannot technically or computationally falsify a valid digital binding.* |

*Object Reuse - SSR19*. [SYSTEM] component systems shall provide safeguards that ensure storage objects contain no residual information from a prior use. Either a "*clear before use*" and/or a "*clear after use*" protective mechanism shall safeguard against unauthorized access to residual information in a storage object. Note, performance penalties may result in choosing either acceptable clearing strategy, but not necessarily both.

*Recovery - SSR20*. [SYSTEM] component systems shall provide recovery capabilities via data archive or other techniques that restore [SYSTEM] functions, replicate functionality-specific data, and protect data against loss. Off-site storage for archived data shall also be provided.

*Virus Protection - SSR21*. [SYSTEM] component systems shall provide virus protection capabilities via software or other techniques that prevent insertion of malicious content code (viruses, Trojan Horses, and the like) into [SYSTEM] file systems (usually via magnetic media such as hard disk drives or diskettes).

**Procedure Security Requirements (PSR)**.

*Access - PSR01*. [SYSTEM] component systems shall establish rules and procedures which control access to [SYSTEM] component system facilities, hosts, terminals, gateways, communications links, software, and applications. System developers shall update existing site access programs to account for [SYSTEM] functionality, message sensitivity, and other functional or legal authorizations (e.g., only a warranted official may approve certain message obligations). Whenever feasible, these rules shall be enforced by automated means (e.g., a motion detector for a gateway computer which operates unattended).

*Accountability - PSR02*. [SYSTEM] component systems shall provide features to establish and maintain required functional and/or legal “chain of custody” rules for message exchanges. Techniques to sequence work through the several stages necessary to approve procurements, solicit responses from associate organizations, review draft contractual documents, or make legally binding awards shall provide for satisfying these rules. Further, other techniques such as archival records, transaction logs, and security audit trail recordings can be effective accountability measures when used in conjunction with established business practices (e.g., help to verify a contract award has a companion solicitation and offeror response).

*Continuity of Operations*.

- Mission Support - PSR03. [SYSTEM] component system features shall support practices and measures taken in support of continuity of operations goals. This includes installing uninterruptible power sources, providing alternative communications circuits, conducting initial and follow-up training, following formal procedures to review events recorded in security audit trails, investigating suspicious system activity, reporting potential and actual security "incidents", and the like.

- Security Administration - PSR04. [SYSTEM] Component System features shall support life-cycle security administration functions. These functions include configuration management for security feature parameters (e.g., the so called "factory settings" to establish basic rules for security feature parameters), managing user authorizations, security training, and identifying certification and accreditation issues resulting from security "incidents," and interaction with the life-cycle Central Design Agency (CDA).

*Documentation*.

- Design Documentation - PSR05. Documentation shall be available that provides a description of the philosophy of protection and an explanation of how security features implement this philosophy.

- End User Manual ( or equivalent content Security Features User's Guide) - PSR06. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the [SYSTEM] security features, guidelines on their use, and how they interact with one another.

- System Administrator's Manual (or equivalent content Trusted Facility Manual) - PSR07. A manual, addressed to the system administrator, shall present cautions about establishing, controlling, and managing functions and privileges when running a secure facility.

**Assurance Security Requirements (ASR)**.

*Accreditation Package - ASR01*. The [SYSTEM] Program Office shall prepare a comprehensive accreditation package for each [SYSTEM] Component System. See [applicable reference documentation], for details on how to assemble the Accreditation Package.

*Certification Package - ASR02*. The [SYSTEM] Program Office shall prepare a comprehensive certification package for each [SYSTEM] Component System. See [applicable reference documentation], for details on how to assemble the Certification Package.

*Sustaining Plans*.

- Certification and Accreditation Plan - ASR03. The [SYSTEM] Program Office shall prepare a comprehensive Certification and Accreditation Plan for each [SYSTEM] Component System. The Plan shall address the Security Disciplines in this Policy and shall provide detailed steps leading to successful certification and accreditation.

- Certification and Accreditation Support Plan - ASR04. The [SYSTEM] Program Office will provide support to all certification and accreditation activities. These activities include security

testing and evaluation, documentation, security discipline certification tests (other than ST&E), and network and external interface testing.

- Configuration Management Plan - ASR05. The [SYSTEM] Program Office and each [SYSTEM] System Administrator shall provide configuration management for [SYSTEM] hardware and software items. Whether accomplished by procedural or automated methods, configuration management processes shall control changes to requirements, specifications, software, hardware, system design, implementation documentation, source code, the running version of object code, test fixtures and documentation, and the like.

- Security Test and Evaluation Plan - ASR06. The Program Office shall prepare for each [SYSTEM] Component System a document describing the security test philosophy, detailed test scripts, and test evaluation criteria. The Program shall also document results from testing the protective security mechanisms and include them in the Certification Package for each [SYSTEM] Component System.

- Security Training Plan - ASR07. Each System Administrator shall provide necessary training so all authorized functional users are familiar with the security behavior of the [SYSTEM] hardware and software platforms. The Program shall also provide Training for Associate System Administrators.

## Appendix B  Policy Descriptions, Security Architecture Concepts

**Disciplines.** Security disciplines for [SYSTEM] stem from guidance in [place relevant policy guidance here], and applicable directives and regulations derived from [place relevant policy guidance here] guidance. Thus, appropriate security measures shall be in a [SYSTEM] context based on these fundamental security disciplines. In turn, protective security measures derived from these disciplines must undergo a comprehensive risk assessment to determine the patent and latent risks associated with applying them in the [SYSTEM] context.

*Communications Security (COMSEC)*. COMSEC guards against disclosing sensitive or classified information on communications circuits by protecting them with cryptographic or other approved techniques.

*Computer Security (COMPUSEC)*. COMPUSEC provides computer-enforced safeguards which protect information manipulated, processed, stored, or otherwise handled in an automated manner. COMPUSEC also provides the mechanisms (i.e., available in a Controlled Access Protection compliant operating system) necessary to permit resource and data sharing among users some of whom may not be permitted to access all available resources, date, or even capabilities.

*Emanations Security (EMSEC)*. Sometimes called by its classic term *TEMPEST*, EMSEC prevents exploiting intercepted electromagnetic energy radiated from equipment that processes sensitive or classified information.

*Information Security (INFOSEC)*. INFOSEC guards against actual or potential information loss through a combination of system-enforced safeguards, administrative policies, and procedures which alert people to a product's sensitivity or classification. It also establishes the need to account for, store, and destroy such information as prescribed by basic information security regulations.

*Network Security (NETSEC)*. NETSEC extends centralized security protection features to networks and their distributed components. Through these techniques, it performs Identification and Authentication (I&A), implements system-enforced access controls that adjudicate granting privileges to accessing systems and users, and audits user activity for network-provided services.

*Operations Security (OPSEC)*. OPSEC denies friendly capabilities and intentions information to hostile intelligence services by identifying, controlling, and protecting indicators associated with planning and conducting military operations and related activities. OPSEC ensures hostile intelligence services cannot satisfy their four basic mission objectives (i.e., detect, recognize, identify, and locate intelligence information).

*Personnel Security (PERSEC)*. PERSEC ensures proper authorization [clearance] for people who require access to sensitive information to perform their official duty tasks.

*Physical Security (PHYSEC)*. PHYSEC wards off intrusion into sensitive or classified work areas by establishing physical control zones that require formally granted permission to enter unescorted.

**Safeguards.** Safeguards are protective measures and techniques derived from the fundamental security disciplines cited above. Usually system-enforced, safeguards include security protection features in operating systems, utilities, communications software, internal and external hardware, cryptographic devices, [SYSTEM] functional applications, and security software. The system shall enforce the following safeguard principles or rules to protect business information handled by [SYSTEM] component systems.

*Access Control*. [SYSTEM] component systems shall implement an access control policy of "***Deny Access Unless Otherwise Explicitly Permitted***". The System Administrator shall grant all users with access to [SYSTEM] component systems appropriate permissions and/or privileges according to their mission task requirements or functions. No person by virtue of rank or position *only* has the right to access or use [SYSTEM] Component Systems. The system shall adjudicate all accesses, whether procedural and/or system enforced, based on having an official duty responsibility in the procurement process. System Administrator(s) shall be responsible for properly configuring access control parameters consistent with this mandatory policy.

*Archive*. [SYSTEM] component systems shall implement an archive policy in support of operational continuity and non-repudiation disputes. The retention period archived records shall satisfy current procurement guidelines (e.g., "n" days on-line, "n" days off-line storage).

*Audit*. [SYSTEM] component systems shall implement a security audit trail recording policy for actions taken during user sessions (e.g., establish personal accountability). Recorded actions are events relevant to security policy rule enforcement and shall indicate event attributes (e.g., date and time of the event, user, type of event, and success or failure of the event). The system shall protect security audit trail mechanisms and recordings from modification, unauthorized access, or destruction.

*Authenticity*. [SYSTEM] component systems shall implement and enforce an authenticity policy for transaction message content (e.g., the exact message content shall be undeniable). Results shall be recorded in the security audit trail.

*Availability*. [SYSTEM] component systems shall implement an assured availability policy. The policy must ensure reliable service is available to authorized users upon demand and result in robust communication paths to ensure there are few, if any, scenarios capable of significantly impacting overall system availability.

*Confidentiality*. [SYSTEM] component systems shall implement and enforce a confidentiality policy which precludes unauthorized access to protected resources (e.g., functional user menu selections, files). Outcomes from confidentiality decision rules reflecting permitted [forbidden] access shall be in the security audit trail.

*Cryptography*. [SYSTEM] component systems must implement a policy to provide encryption for functional area data exchanged among [SYSTEM] sites, the [SYSTEM] gateways, or other system(s) used for [SYSTEM] purposes. Cognizant organizations shall approve all cryptographic devices prior to placing them in operational service. The Program shall provide a cryptographic Key Management System and supporting infrastructure for [SYSTEM] component systems. Cryptographic device(s) and Key Management System(s) the Program uses in the [SYSTEM] context shall evolve and remain compatible with their organizational counterparts.

*Identification and Authentication*. [SYSTEM] component systems shall implement and enforce an identification and authentication policy requiring users to identify and authenticate themselves prior to gaining further access. The system shall protect Identification and Authentication features and associated parameters from unauthorized modification or access.

*Integrity*.

a. Information Integrity. [SYSTEM] component systems shall implement and enforce an information integrity policy ensuring all protected data changes occur in a specified and authorized manner. Information integrity features shall safeguard against computer viruses or other malicious software entities. Configuration management and other procedural methods shall

support the integrity of the functional user community's data files, records, pending actions, and so on.

b. System Integrity. [SYSTEM] component systems shall provide hardware and/or software mechanisms that periodically validate the correct operation of the security features implemented in site hardware or firmware.

*Interfaces*. [SYSTEM] component systems shall implement and enforce resource sharing policies for internal interfaces (between and among entities residing on the same computer) and for external interfaces (between and among entities residing on different computers).

a. External Interfaces. [SYSTEM] component systems shall provide interface capabilities to internal, functionally-related interfaces to securely handle inter-application resource sharing (e.g., interprocess communications techniques).

b. Internal Interfaces. [SYSTEM] component systems shall provide interface capabilities to external computer systems to securely handle file transfers, contracting transactions, and other applicable resource sharing functions.

*Markings*. [SYSTEM] component systems shall implement and enforce a policy of marking displays and output products when required by statute, law, or regulation. Such markings shall alert viewers about the restrictive handling or access limitations the Program must apply to ensure the confidentiality of information (e.g., a terminal screen or hard-copy report that includes Privacy Act data).

*Non-Repudiation*. [SYSTEM] component systems shall implement and enforce policies prescribed by non-repudiation rules. Three non-repudiation rules for [SYSTEM] are:

a. Non-Repudiation of Origin. Strong digital evidence binding the identity of a party originating a transaction message and the exact contents of the message.*

b. Non-Repudiation of Receipt. Strong digital evidence binding the identity of a party receiving a transaction message and the exact contents of the message, and *

c. Trusted Time Stamp. Strong digital evidence binding the time-of-event of a transaction message to the exact contents of the message.*

**Any alteration, deletion, addition, or misrepresentation shall be detectable and provable to an impartial third party. Thus, a valid digital binding must be technically or computationally impossible to falsify.*

*Object Reuse*. [SYSTEM] component systems shall implement and enforce an object reuse policy upon reusable storage objects (e.g., main memory buffers in a computer).

*Recovery*. [SYSTEM] component systems shall implement a policy leading to assured recovery of mission capabilities and data archive in the event of a contingency (e.g., a power failure, computer peripheral failure). The Program shall consider both computer-based and procedure-based techniques when developing recovery plans and actions.

Procedures. The next architecture concept moving toward the goal of system accreditation is the procedural-based policy needed for safeguarding data system processors, their peripherals, the [SYSTEM] gateway, and remote terminals (if any). These techniques provide further rules necessary to configure and control the computer system safeguard mechanisms, as necessary, to meet overall security policy goals.

The Program must certify all procedures for their sufficiency to protect the sensitive (or classified) information entrusted to [SYSTEM] component systems.

*Access*. The [SYSTEM] Program shall implement a policy of establishing rules and procedures which control access to [SYSTEM] component system facilities, hosts, terminals, communications gateways, communications links, software, and applications. Whenever feasible, the system shall enforce these rules by automated means (e.g., provide a motion detector for an unattended gateway computer).

*Accountability*. The [SYSTEM] Program shall implement and enforce an accountability policy for transaction message exchanges to safeguard against loss of functional or legal accountability requirements. Rules for accountability practices shall be formally documented in the End User's Manual.

*Continuity of Operations*.

a. Mission Support. The [SYSTEM] Program must implement a policy of sustaining mission support throughout the Program's life-cycle (e.g., redundant peripherals, alternate communications links, management oversight of on-going functional activities).

b. Security Administration. The [SYSTEM] Program must implement a policy of establishing and sustaining security administration functions throughout the Program's life-cycle (e.g., configuring security parameters per "factory settings" given in release notices, training for Associate System Administrators).

*Documentation*. The [SYSTEM] Program shall pursue a policy of maintaining sufficient security documentation to properly support operations, security concepts and policies, user interaction with the functional application(s), System Administrator activities, gateway procedures and operation, and so on—in short, system documentation illustrating the security behavior of [SYSTEM] component systems. At a minimum, the documentation shall include a System Administrator's Manual (or equivalent "Trusted Facility Manual" content), an End User's Manual, or (equivalent "Security Features User's Guide" content).

**Assurances.** These are the measures taken to ensure [SYSTEM] component system security protection measures are sufficient for informed decisions leading to operational deployment via the certification and accreditation processes.

*Accreditation Package*. The [SYSTEM] Program shall support a policy of formally accrediting the sufficiency of security protection features as implemented and configured for the operational environment. Cognizant Designated Approving Authority(ies) shall approve or disapprove [SYSTEM] component system for operational use. The DAA(s) (Designated Approving Authority) will review the results from the certification package (e.g., risk survey, results from security test and evaluation, residual risk statement) to validate whether or not [SYSTEM] component systems meet the technical security requirements of the functional area mission. If these security protection features provide the requisite protection for sensitive functional area information, then the DAA(s) will accredit [SYSTEM] component systems for the operational environment.

*Certification Package*. The [SYSTEM] Program shall support a policy of formally certifying [SYSTEM] component systems in their intended operational environment. Specifically, the Program will formally certify security functions, features, and techniques for functionality, appropriateness, and correct implementation. In turn, certifying officials shall document and make available tests results, analyses, or vendor-provided certificates for review and validation by cognizant Designated Approving Authority(ies).

*Sustaining Plans*. The [SYSTEM] Program shall support a policy to formalize and publish plans that sustain certification and accreditation. The required plans include, but not limited to: Certification and Accreditation Plan, Security Test and Evaluation Plan, Security Training Plan, Configuration Management Plan, and/or Contingency Plan.

# Appendix C  Concept of Operations

**Mission.**

Application Systems.  The [SYSTEM] architecture calls for application systems running on [SYSTEM] component systems to process (functional) community information needed for [SYSTEM] business activities (example here).  The specific business data will use transaction messages, in conjunction with (example here) implementation conventions for those standards.  Organizational component systems sites will use the DoD, Federal, and commercial networks to transmit business data to (example here) for [SYSTEM] services (translation, directory, communications, and security).

Gateway.  The [SYSTEM] architecture also calls for Gateways to perform (example here) transaction processing such as translation, enveloping, archive and/or retrieval, encryption, and security.  The Gateway must also provide the necessary technical and operational support to accept and route transactions from outlying sites for outbound transactions.  In turn, gateways will support "one-to-many" transaction broadcasts to appropriate networks using DoD, federal, and commercial networks.  For inbound transactions, the network interface point will route transactions to the appropriate [agency] site(s) via [agency] Gateways.  Data archiving features must provide recovery capability and retransmission within (n) hours of request by the networks, contractors, or [agency] site.  Primary archive and retrieval responsibility rests with the creator of the initial data (agency or contractor).

**Communications.**

Connectivity to DoD and commercial networks, message handling functions, cryptographic methods, and inbound and outbound transaction handling techniques form the core of the communications requirements for [SYSTEM].  DoD and the (agency) follow International Telecommunications Union - Telecon Standard Sector (ITU-TSS, formally CCITT) X.400 Communications, Government Open Systems Interconnected Profile (GOSIP), and ITU-TSS X.500 Directory Services as addressing and communication standards for agency-wide use.  Capabilities will be needed to handle X.400-addressed messages.  Furthermore, agency X.400 technologies will need to comply with DoD Messaging System (DMS) architecture.

**Data Encryption.**

Support for encryption devices supporting digital signatures, message digest functions, and trusted time stamp are examples of future requirements.  However, the details and exact mechanisms are presently unclear (e.g., which FORTEZZA technology variant will be used).

**Operational Security Considerations.**

The following paragraphs describe the operational security considerations within the [SYSTEM] security environment. This environment includes [SYSTEM] facilities, authorized contracting personnel, user workstations, the functional host systems, functional applications, the agency Gateways, and the communications circuits involved.

**Facility, Personnel, and Maintenance Rules.**

*Facility Rules*. [SYSTEM] facilities shall provide a physical security environment that protects computer systems and associated resources from natural and physical disasters, human threats, and other identified physical threat agents. Needed physical security measures include establishing Controlled Access Areas, implementing entry controls, and providing backup storage.

*Personnel Rules*. Personnel security consists of policies and procedures guiding the ethical and official duty conduct. While a security clearance is not now mandatory for [SYSTEM], all users must have a verified need-to-know for all data they can access. [SYSTEM] System Administrators shall make the need-to-know determination based upon an access requested by the user's supervisor. In addition, the Program must brief users that behavior contrary to established security policy rules may result in sanctions (e.g., denying access to [SYSTEM] systems or capabilities). More importantly, users must have written guidance about their responsibilities to protect [SYSTEM] component system resources (e.g., via an End User's Manual).

*Maintenance Rules*. The Program shall only use approved procedures (e.g., those specified in vendor maintenance publications) to maintain equipment and software components. Trained personnel shall supervise or directly maintain these components. In addition, maintenance technicians must periodically check and formally document whether unauthorized modifications have occurred.

**User Interface Rules.** Passwords and user_IDs are critical attributes necessary to identify and authenticate the [SYSTEM] user interface. The following rules highlight the importance of properly managing these attributes:

a. The Program will conveniently construct user_IDs to readily associate a person with his or her user_ID (e.g., the Branch, Section, Person (BSP) scheme used in [SYSTEM] is a sound approach). [SYSTEM] component systems shall limit the number of consecutive incorrect access attempts by a user_ID to no more than (n) - automatically deactivate the user_ID after the (nth) consecutive unsuccessful logon attempt.

b. The system must construct passwords with sufficient random characteristics to preclude a ready guess (e.g., not a dictionary word or variant thereof). In no instance shall passwords be fewer than (n) characters.

c. The Program must implement password aging to keep passwords consistent with functional user activity (e.g., must "expire" at least once every "n" days, help detect dormant accounts).

d. The system must protect passwords from tampering and from unauthorized viewing (e.g., always stored in an encrypted form).

**Idle Time Management.** [SYSTEM] component systems shall generate automatic time-outs for connected terminals when inactivity exceeds (n) minutes. System Administrators may modify time limits

on a case-by-case basis when operational requirements dictate otherwise. Note that time-outs do not necessarily lock out the user - another logon should reestablish connection.

**Privately Owned, Public Domain, and Shareware Software Rules.**

*Privately Owned Software Rules*. As used here, the term *software* refers to operating system, applications, communications, security, and utility software, to include database, spreadsheet, and word processing applications. No one shall load or execute privately owned software on [SYSTEM] component systems. For personally written or locally developed software, a trusted programmer or analyst shall examine code, compile the program on a trusted Government machine, and obtain formal DAA approval prior to installation.

*Public Domain Software and Shareware Rules*. No one shall install public-domain software or shareware on an [SYSTEM] component system without obtaining formal, ***written*** DAA approval to do so.

Continuity of Operations Planning. The [SYSTEM] Program Office shall develop a Continuity of Operations Plan (COOP) to reduce the impact caused by unanticipated interruption of an organizational component system operation. The COOP shall establish procedures to follow if a catastrophic event happens, how to reduce the impact from such events, and how to resume operations after the event. The plan shall address natural and system events. [place applicable documentation reference(s) here], provide contingency planning guidance.

Fraud, Waste, and Abuse. [Place applicable documentation reference(s) here], formalizes the organizational commitment to prevent and eliminate fraud, waste, and abuse. It prescribes policy, establishes procedures, and provides guidance to make sure allocated organizational resources support national priorities. [SYSTEM] component system users and managers at all levels shall support fraud, waste, and abuse policies. Additionally, no users shall violate copyright laws (specifically software and software documentation). Everyone must be aware of and abide by copyright restrictions placed on automated system software.

**Training and Awareness.** Training shall promote proper and consistent adherence with rules about [SYSTEM] component systems security features and procedures that protect sensitive information. The [SYSTEM] training program shall address reporting incidents and vulnerabilities under the Computer Security Technical Vulnerability Reporting Program (CSTVRP). (See [place applicable documentation reference(s) here], for additional guidance.)

## Appendix D Security Features to Architecture Element Mapping

**Allocations.** Table 1 lists the [SYSTEM] component system architecture elements that will implement the security requirements given in Section 4. It also gives the coding scheme used in Table 3.

| | | **[SYSTEM] Component System Architecture Elements** |
|---|---|---|
| *Table 3 Code* | *Full Title* | *Synopsis Description* |
| *Apps* | Applications | A generic reference to all functional applications programs that collectively provide support to the functional community. |
| *Comm Pkgs* | Communications Packages | Specialized programs that provide communications capabilities (e.g., File Transfer Protocol (FTP)). |
| Facility | [SYSTEM] Facilities | The building, rooms, and other physical structures that house [SYSTEM] component systems. |
| Gateway | Organizational gateway | An intermediate message switching system between the organizational [SYSTEM] host computers at the several sites and the network entry point. |
| Host | [SYSTEM] Host Computers | The computer, mass storage devices, peripherals, communications interface devices, and so on that collectively support [SYSTEM] functional applications. |
| OS | Operating System | The computer operating system for the [SYSTEM] computers (e.g., IBM, UNIX). |
| Proc | Procedures | The administrative and procedural measures necessary to operate and maintain mission capabilities for the functional area community. |
| Prog Mgt | Program Management | The organization and infrastructure responsible for fielding and providing life-cycle support for the [SYSTEM] Program. |
| Sec Pkgs | Security Packages | Specialized programs which provide Controlled Access Protection functionality (e.g., ACF2). |
| Utility | Utility Packages | A generic reference to word processors, spreadsheets, editors, and other software used in conjunction with functional applications. |
| WS | Work Stations | A generic reference to the functional user's terminal and adjacent work place. |

Table 1, [SYSTEM] Component System Architecture Elements

**Allocation Mapping Rationale.** Table 2 shows the rationale for allocating security requirements to [SYSTEM] component system architecture elements.

| Requirement | Allocation Mapping Rationale |
|---|---|
| DSR01 - Communications Security | • Mandatory security discipline for basic security requirements. |
| DSR02 - Computer Security | • Mandatory security discipline for basic security requirements. |
| DSR03 - Emanations Security | • Mandatory security discipline for basic security requirements. |
| DSR04 - Information Security | • Mandatory security discipline for basic security requirements. |
| DSR05 - Network Security | • Mandatory security discipline for basic security requirements. |
| DSR06 - Operations Security | • Mandatory security discipline for basic security requirements. |
| DSR07 - Personnel Security | • Mandatory security discipline for basic security requirements. |
| DSR08 - Physical Security | • Mandatory security discipline for basic security requirements. |
| SSR01 - Discretionary Access Control | • Read, write, and execute privileges for each user and permitted access to protected resources (e.g., files).<br>• Privileged menu selections and other access controls based on rules in tables containing user profile information.<br>• Mechanisms implemented via the hardware ports located either on system boards or on individual I/O cards. |
| SSR02 - Security Profile Tables | • Tables for user registration information (e.g., user_ID and passwords).<br>• Tables for file system(s) access privileges and modes.<br>• Tables for directory structure access privileges and modes.<br>• Tables for file access privileges and modes.<br>• Tables for port access privileges and modes.<br>• Tables for menu tailoring access privileges and modes. |
| SSR03 - Archive | • Rules and modules to “safe store” transactions, message exchanges, and the like. |
| SSR04 - Audit | • Operating system’s Security Audit Trail function.<br>• System Administrator established configuration for Security Audit Trail recording options.<br>• Rules for selective security-related event recording. |
| SSR05 - Authenticity | • Rules and authenticity mechanisms (e.g., Message Digest Function) to affirm precise message content. |
| SSR06 - Availability | • Functions for sustaining required operational mission capabilities during the normal business day. |
| SSR07 - Confidentiality | • Rules enforcing user access profile privileges and modes.<br>• Rules enforcing file access privileges and modes.<br>• Rules enforcing program access privileges and modes.<br>• Rules enforcing port access privileges and modes. |
| SSR08 - Cryptography Devices | • Modules handling cryptographic algorithms.<br>• Encryption for transaction message exchanges. |
| SSR09 - Key Management System | • Required to support cryptographic systems. |
| SSR10 - Identification and Authentication | • Rules for user_IDs and passwords (e.g., form, length, randomness).<br>• Rules for password management (e.g., aging, changing, storing). |

| Requirement | Allocation Mapping Rationale |
|---|---|
| SSR11 - Information Integrity | • Rules and formats for transaction message translations.<br>• Edit and format rules.<br>• Data-change authorization rules. |
| SSR12 - System Integrity | • Diagnostics periodically validate on-site hardware and firmware elements of security features. |
| SSR13 - External Interfaces | • Rules for permitted and forbidden external interface exchanges.<br>• Rules for permitted and forbidden resource sharing. |
| SSR14 - Internal Interfaces | • Rules for permitted and forbidden interactions between applications software modules such as [SYSTEM].<br>• Rules for permitted and forbidden resource sharing. |
| SSR15 - Markings | • Capabilities to mark output products with labels indicating Privacy Act, Vendor "confidential," and other commercial identification. |
| SSR16 - Non-Repudiation of Origin | • Rules and modules for handling digital signature at transaction message origin.<br>• Rules and modules that verify claimed origin. |
| SSR17 - Non-Repudiation of Receipt | • Rules and modules for handling digital signature at transaction set message receipt.<br>• Rules and modules that verify claimed receipt. |
| SSR18 - Trusted Time Stamp | • Rules and modules handling trusted time stamp.<br>• Rules and modules that verify claimed time stamp. |
| SSR19 - Object Reuse | • Operating system's object reuse function.<br>• Purging and clearing utility programs. |
| SSR20 - Recovery | • Transaction logging functions.<br>• Modules handling backup, archiving, and transaction logging.<br>• Hardware support [magnetic media drives]. |
| PSR01 - Access | • Facility access control rosters.<br>• Personal security authorizations [clearances].<br>• Badge systems identify individual people. |
| PSR02 - Accountability | • Rules for marking, handling, storing, and destroying Privacy Act, Vendor "confidential," other sensitive but unclassified information, or classified data. |
| PSR03 - Mission Support | • Provides for mission continuity over system failures<br>• Cites procedures to minimize mission impacts due to contingency situations. |
| PSR04 - Security Administration | • Rules for establishing the initial secure operating environment ("factory settings" for security feature enforcement mechanisms).<br>• Rules for properly superintending user accounts, privileges, and access modes.<br>• Rules for properly superintending interface "accounts," privileges, and access modes.<br>• Rules for sustaining security on a life-cycle basis. |
| PSR05 - Design Documentation | • Gives security protection philosophy.<br>• Specifies parameters for security features. |

| Requirement | Allocation Mapping Rationale |
|---|---|
| PSR06 - Security Features User's Guide | • Functional user security responsibilities.<br>• Procedures for using provided security measures.<br>• Precautions about potential security hazards. |
| PSR07 - Trusted Facility Manual | • System Administrator security responsibilities.<br>• Procedures for establishing and maintaining secure operating environment. |
| ASR01 - Accreditation Package | • Authorizes operation in a mission environment.<br>• Acknowledges risks at an acceptable level. |
| ASR02 - Certification Package | • Provides "proof" security measures technically meet established rules. |
| ASR03 - Certification and Accreditation Plan | • Cites methodology for preparing certification and accreditation packages.<br>• Captures individual methodology step outcomes. |
| ASR04 - Certification and Accreditation Support Plan | • Identifies resources and planning for certification and accreditation. |
| ASR05 - Configuration Management Plan | • Prescribes formal configuration controls for security features and functions. |
| ASR06 - Security Test and Evaluation Plan | • Cites approach for conducting security testing.<br>• Prescribes scenarios and expected results. |
| ASR07 - Security Training Plan | • Provides for initial security training.<br>• Provides for security training refreshment.<br>• Addresses functional user security training.<br>• Addresses System Administrator security training. |

Table 2, Security Requirements Allocation Rationale

**Allocation Mapping Summary.** Table 3 summarizes the security requirements allocated to [SYSTEM] component system architecture elements.

| | **[SYSTEM] Component System Architecture Elements** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Requirement** | *Apps* | *Comm Pkgs* | *Facility* | *GW* | *Host* | *OS* | *Proc* | *Prog Mgt* | *Sec Pkgs* | *Utility* | *WS* |
| DSR01 | | | X | X | X | | | | | | X |
| DSR02 | X | X | | X | | X | | | X | X | X |
| DSR03 | | | X | X | X | | | | | | X |
| DSR04 | | | X | | | | X | X | | | |
| DSR05 | X | X | X | X | X | | | | X | | X |
| DSR06 | | | X | | | | | X | | | X |
| DSR07 | X | X | X | X | X | X | X | X | X | X | X |
| DSR08 | | | X | X | X | | X | X | | | X |
| SSR01 | X | X | | | | X | | | X | X | X |
| SSR02 | X | X | | | | X | X | | X | | X |
| SSR03 | X | | X | X | X | X | X | | | X | X |
| SSR04 | | | X | X | | X | X | | X | X | |
| SSR05 | | | | X | X | X | | | X | X | X |
| SSR06 | | | X | X | X | | X | | | | X |
| SSR07 | | X | X | X | | X | X | | X | | X |
| SSR08 | | X | X | X | X | | | | | | X |
| SSR09 | | | X | X | X | | | | | | X |
| SSR10 | | X | X | X | | X | X | | X | | X |
| SSR11 | | X | X | X | X | X | X | | X | | X |
| SSR12 | | | X | X | X | | X | X | X | | X |
| SSR13 | | X | | X | X | | | | | | X |
| SSR14 | X | | | | | X | | | X | | X |
| SSR15 | X | | X | X | X | X | X | | X | X | X |
| SSR16 | | | | X | X | | | | X | | X |
| SSR17 | | | | X | X | | | | X | | X |
| SSR18 | | | | X | X | | | | X | | X |
| SSR19 | X | X | | | | X | X | | X | X | X |
| SSR20 | X | X | X | X | X | X | X | | | X | X |
| PSR01 | | | X | X | X | | X | X | | | X |
| PSR02 | X | | | | | X | X | | X | | X |
| PSR03 | | | X | X | X | | | | | | X |
| PSR04 | X | X | X | X | X | X | X | X | X | X | X |
| PSR05 | X | X | | | | X | | | X | X | |
| PSR06 | X | | X | X | | | X | X | X | | X |
| PSR07 | X | X | X | X | X | X | X | X | X | X | X |
| ASR01 | X | X | X | X | X | X | X | X | X | X | X |
| ASR02 | X | X | X | X | X | X | X | X | X | X | X |
| ASR03 | X | X | X | X | X | X | X | X | X | X | X |
| ASR04 | | | X | X | X | | | X | | | X |
| ASR05 | X | X | X | X | X | X | X | X | X | X | X |
| ASR06 | X | X | X | X | X | X | X | X | X | X | X |
| ASR07 | X | X | X | X | X | X | X | X | X | X | X |

Table 3, Security Requirements Allocation Summary

τΩ Engineering, Inc.

# SECURITY POLICY

TARGET, CONTENT, & LINKS

τΩ

# OVERVIEW

- INTRODUCTION
- POLICY TARGET
- POLICY CONTENT
- POLICY IMPLEMENTATION
- POLICY LINKS
- SUMMARY

τΩ

# INTRODUCTION

- DEFINITION
- LACK OF DEFINED POLICY
- PURPOSE
- HIGH-LEVEL CONTENT
- DETAILS IN SFUG & TFM

τΩ

# POLICY TARGET

- WHO IS THE AUDIENCE?
- HIGH-LEVEL PERSPECTIVE
- FINANCIAL & TECHNICAL JUDGMENTS
- GAINING SUPPORT

τΩ

# POLICY CONTENT

- HIGH-LEVEL SECURITY RQMTS
- POLICY DESCRIPTIONS
- CONCEPT OF OPERATION (CONOPS)
- ARCHITECTURE ELEMENT ALLOCATIONS

τΩ

# POLICY IMPLEMENTATION

- **END USER MANUAL** (or like content Security Features User's Guide-SFUG)
- **SYSTEM ADMINISTRATOR'S MANUAL** (or like content Trusted Facility Manual-TFM)

τΩ

# POLICY LINKS

- SENSITIVITY, CRITICALITY, VULNERABILITY
- BUSINESS PROCESSES
- SECURITY ARCHITECTURE
- SECURITY MODELS
- SECURITY RQMTS & SPECS
- SOFTWARE DESIGN
- TEST PROCEDURES

τΩ

# SUMMARY

- **SENIOR-LEVEL MANAGER TARGET**
- **POLICY CONTENT**
  - REQUIREMENTS
  - DESCRIPTIONS
  - CONOPS
  - ALLOCATIONS
- **POLICY IMPLEMENTATION**
- **POLICY LINKS**

τΩ

# QUESTIONS

?