NISTIR 4614

Standard Security Label for GOSIP An Invitational Workshop

Noel Nazario
Chairman

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4614

Standard Security Label for GOSIP An Invitational Workshop

Noel Nazario
Chairman

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

June 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Table of Contents

Abstract

On April 9 and 10, 1991 the Protocol Security Group at NIST held its Second Workshop on Security Labels. Forty representatives from the U.S. Government, Industry, and the Canadian Government gathered for two days to discuss a NIST proposed Standard Security Label for the U.S. Government Open Systems Interconnection Profile. Issues on security policy and security object registration were also discussed in reference to the proposed label. The information shared during the two days of discussion and the recommendations of the group are documented in these proceedings.

Key Words: Government Open Systems Interconnection Profile (GOSIP); Computer Security Objects Register; Open Systems Interconnection; security labels

Papers are contributions of the authors and do not necessarily represent NIST views.

Workshop Report

Robert Rosenthal, Manager of the Protocol Security Group at NIST, welcomed the attendees. He described the role of this workshop in NIST's effort to incorporate security mechanisms into the U.S. Government Open Systems Interconnection Profile. Mr. Rosenthal envisions a set of Government OSI Security Profiles that will be pointed to by the Federal Information Processing Standard (FIPS) 146, GOSIP. The first set of profiles would include the following topics:

- Key Management for Public Key Cryptography
- Security Protocol for Layer 4 (SP4)
- Security Labels
- Cryptographic Modules
- Register for Uniquely Named Managed Security Objects

Mr. Rosenthal introduced Noel Nazario (NIST), Workshop Chair. Mr. Nazario reviewed the agenda and asked the attendees to introduce themselves. Appendix A contains a list of attendees.

Larry Keys (NIST), will be the Registrar for NIST's Computer Security Objects Register (CSOR). The CSOR is being organized using ANSI/ISO guidelines for object registration. Mr. Keys gave a status report on the work done so far in setting up this service and outlined the basics of the registration procedure.

George Rogers (IC Staff) asked whether this register could or would register classified objects. Dr. Dennis Branstad (NIST) answered that NIST has no authority over classified information. Branstad added that since the register deals with a hierarchical structure the "classified side" could be treated as a branch of the same tree structure. Mr. Rogers expressed concern with having more than one register and recommended avoiding this situation if possible.

Dr. Stuart Katzke (NIST) spoke about the relationship between security labels and data categorization. Data is categorized according to the protection required thus reflecting the risks involved in their loss and misuse. Some issues in this area are:

Types of categories: Confidentiality, Integrity, Availability

Structural relationship between categories: Hierarchical (e.g., DoD Model for Confidentiality), Lattice, Independent.

Independence between data categorization structure and access control models such as Access Control Lists, Bell and LaPadula/Clearances, Capabilities, Chinese Wall, and Biba. Interpretation of categories as they relate to protection objectives. (e.g., No consensus on an interpretation of hierarchical integrity categories.)

Implementation and enforcement of data categorization policy.

- Protection Objectives vs Mechanisms
- Consistent interpretation of protection objectives by the organization receiving the data.
- Variation of protection objectives based upon organization receiving the data. (e.g., Modification may be done by agency X while only read access is permitted to agency Y)

Ancestry: How much needs to known about the data's generation, change, and disposition ancestry to protect them properly. What are the protection requirements on this ancestry information.

Dr. Katzke gave a historical perspective of efforts made in addressing the data categorization problem. Some important events were:

Work was initiated at NIST in the early 70s by Branstad and Katzke.

Subcommittee on Automated Information Systems Security/National Telecommunications and Information System Security Committee (SAISS/NTISSC): Their work resulted in coining the term "Sensitive Unclassified".

Computer Security Act: Adopted the term "Sensitive Unclassified". The act gave no guidance for determining the degree of sensitivity.

Computer and Telecommunications Security Council (CTSC): Warren Schmitt presented to the CTSC his categorization model. This model consists of three levels (Low, Medium, High) along three axes (Confidentiality, Integrity, Availability). The resulting matrix is then mapped to the appropriate mechanisms.

NIST's First Invitational Workshop on Security Labels for Open Systems was held on May 30 and 31, 1990. The proceedings were published as NISTIR 4362.

Computer Systems Security and Privacy Advisory Board: Presentations on Data Categorization Requirements and Approach based on initiatives by:

- Canadian Government
- Drug Enforcement Community
- Specific Federal Agencies (e.g. Census Bureau, IRS, Matching Programs)
- Federal Agencies under Bilateral Agreements

So far all discussions on the subject have lead to "black holes" (i.e., No general agreement has been achieved). Potential actions

that could result in uniform data categories for the federal government include:

- Office of Management and Budget (OMB) policy decisions

- Congressional legislation

- Selection of categories within major Department of Defense efforts such as the Corporate Information Management (CIM) and/or Computer-aided Acquisition and Logistics Support (CALS).

Dr. Katzke concluded his presentation by recommending that this workshop focus on the less controversial part of the problem (i.e., Agreeing on a label format).

Noel Nazario (NIST) summarized the developments in the labeling effort since the previous workshop. These include:

The publication of the proceedings of the May 1990 labeling workshop as NISTIR 4362, "Security Labels for Open Systems an Invitational Workshop."

A panel session at the 13th National Computer Security Conference chaired by Dr. Dennis Branstad (NIST). This session included the participation of Russ Housley (Xerox), Warren Schmitt (Sears Technology Services), and Noel Nazario (NIST).

The release for comment of an initial proposal for a security label based on the output of the first labeling workshop.

Interaction with the Trusted Systems Interoperability Group (TSIG), developers of the Commercial Internet Protocol Security Option (CIPSO).

Presentation on NIST's GOSIP labeling effort at the Workshop on Database Security Labeling for Civilian Agencies in Tucson, Arizona.

The decision by NIST to establish and maintain a Computer Security Objects Register (CSOR).

The release for comment of the initial draft of a Federal Information Processing Standard (FIPS) specifying a Standard Security Label for the Government Open Systems Interconnection Profile.

Ron Sharp (AT&T) represented the Trusted Systems Interoperability Group (TSIG). Mr. Sharp described the TSIG as a very informal group of implementors interested in developing interoperable trusted distributed systems. The TSIG is engaged in projects such as CIPSO, Trusted X-Windows, Trusted Network File Systems (NFS), Trusted Session Management, and Trusted Sockets. The current focus for TSIG members is the TCP/IP communications protocol but the door remains open for a transition to OSI as markets emerge. In developing CIPSO the TSIG adopted and modified original work done by Sun Microsystems and Hewlett-Packard. The group has spawned an Internet Working Group whose purpose is to present CIPSO as an Internet Request for Comment (RFC). Mr. Sharp enumerated reasons for the development of CIPSO, its main features, and presented the label format. His presentation slides and the current version of the CIPSO specification appears on page 55 of this document.

Noel Nazario presented the Standard Security Label (SSL). The specification for this label is given by the initial draft of a FIPS, called Standard Security Label for the Government Open Systems Interconnection Profile. This document provides the format of a security label that may be used at different layers of the OSI architecture. The semantics of the label will be given by a Computer Security Objects Register (CSOR). This future FIPS will be referenced by the U. S. Government Open Systems Interconnection Profile (GOSIP) when describing labeling options for various protocols.

The SSL begins with a Security Label Indicator and a length field indicating the length of the Security Information that follows. The Security Information field includes a Register Index Code (RIC), a Security Level field, and Security Tags. The RIC identifies the semantic rules for the label as registered in the CSOR. There are four tag types, one of which indicates the end of the label. The other three tag types may be used to carry additional security information. The presentation slides on page 21 of this report illustrate the general format of the label and the four tag types. A full description appears in the draft FIPS text also included.

Mr. Nazario compared the label option currently specified by GOSIP for the Connectionless Network Protocol (CLNP) to the SSL. The GOSIP CLNP security option is actually two separate options defined by two different authorities or activities while the SSL can provide the same information in a label defined by a single authority. The Classification Protection Level in the Basic Security Option (BSO) is analogous to the Security Level field in the SSL. The equivalent of the Additional Security Information in the Extended Security Option (ESO) can be provided by the three information-carrying tag types in the SSL.

Mr. Nazario also compared the SSL to the Commercial CIPSO. There are two main distinctions between the CIPSO label and the SSL. The Domain of Interpretation field that identifies the defining authority for the CIPSO label is a four octet fixed length field while the RIC, which points to the semantics of the label as registered in the CSOR for the SSL, is a variable length field. The second difference is that every CIPSO tag has a security level field while there is only one security level field in the SSL.

Noel Nazario also presented proposed modifications to the text in the security chapter (6) of the U.S. Government Open Systems Interconnection Profile (GOSIP). Chapter 6 of GOSIP currently contains the specification for a security option for the Connectionless Network Protocol (CLNP). This chapter is also a placeholder for future specifications. Changes include a new paragraph structure to accommodate a NIST Security Information option for CLNP and placeholders for security parameters at other layers. Only a label parameter is currently defined within the NIST Security Information option. A pointer to the SSL document provides the format specification for this label parameter. The new text also points to the Computer Security Objects Register (CSOR) to provide the semantics for the label. The new CLNP Security Parameter allows the use of either the existent BSO/ESO label or the NIST Security Information. The BSO/ESO was kept for backwards compatibility.

Wayne Jansen (NIST) presented an overview of Security Labels at the Transport Layer. His discussion dealt with the Transport Layer Security Protocol (TLSP). The TLSP, currently under development within ISO, is being balloted for CD (Committee Draft) status. Mr. Jansen compared the SSL and the TLSP label formats and their respective views on label registration. The presentation suggested a compromise format for the alignment of both labels and a methodology for creating label definitions independent of encoding concerns using ASN.1.

Russ Housley (Xerox) presented comments on the draft Standard Security Label document. The proposed label may be applicable to several protocols within the OSI architecture. However, an ASN.1 definition would be necessary for use at layer 7. The IEEE 802.2 working group is currently working on a layer 2 label, it would be appropriate to present the SSL to that group. Mr. Housley added that there should be a reference in the SSL text that indicates what document provides usage rules for this label. The full text of the Xerox comments appear later in this document.

Hilary Hosmer (Data Security) presented the concept of multipolicy. She pointed out that OSI security labels should be able to support co-existing security policies . Ms. Hosmer stated that allowing only one Security Level field in the SSL is a serious limitation because it makes it difficult to support multiple security policies.

David Crawford (Canadian Defense) discussed Canada's coexisting security policies. He explained the relationship between security levels that cover the equivalents to U.S. Classified and Unclassified but Sensitive.

Thomas Bartee (IC Staff) presented a position paper justifying a request for an additional tag type for the Standard Security Label (SSL). Mr. Bartee's argument was that the tags currently specified in the SSL are geared towards indicating restriction markings. The addition of a "reversed" bit map type would make it easier to specify permissive markings such as release indicators. He mentioned that such an approach is currently used in the Director of Central Intelligence Office (DCI) Extended IP Security Option and by the Compartmented Workstation program.

Most of the second day of the workshop was devoted to discussion of issues raised in the presentations of the first day. The group listed and prioritized the different issues. This ordered list guided the discussion of the relevant topics. After discussing each issue an informal vote was taken. The position taken by the group was recorded as the workshop's output. That output is presented in the following section.

Workshop's Output

The following list of issues were identified and discussed by the workshop attendees. The statements listed under each issue were subject to an informal vote and represent the group's position. This list constitutes the workshop's output.

Scope

The option to expand sizes and add tag types should be left open.

Focus the use of labels at layers 3, 4, 2 and 7.

It should be specified that the ASN.1 definition provided applies to layer 7 while the format given in the SSL document applies to layers 3, 4, and 2.

Usage of Labels

The Usage section in the SSL document should specify that the label applies to the data unit.

The Usage section should include a pointer to the source for exception processing rules.

Register Index Code

Given that the length of the Index will always appear after the label Indicator the RIC Indicator should be eliminated.

Length value 255 should be reserved for future use.

Security Level Field

The Security Level field should be eliminated in favor of a Security Level Tag Type.

Multiple Labels

A single label with multiple RIC-tag sets should be allowed as opposed to multiple labels.

Lengths

No multi-octet length fields should be allowed for layers 2, 3, and 4.

All [tag] lengths should be allowed to go up to 255.

Placing of the SSL within GOSIP

The use of BSO/ESO should be mutually exclusive with the NIST Security Information [in CLNP].

BSO/ESO should only be supported by CLNP [for backwards compatibility].

Null Tag

The Null Tag Type should be eliminated.

An additional length field should be used to support multiple RIC-tag sets.

Definitions

Usage of terms should be revised for consistency and all definitions should be included in the document.

Other

A tag type for permisive functionality should be added.

The Standard Security Label should provide for multiple instantiations of RICs followed by their respective tags.

Workshop Contributions

"Government OSI Security Profiles" (Presentation Slide), Robert Rosenthal (NIST)

Government OSI Security Profiles

		FIRST PROFILE	FUTURE PROFILES
Protocols	Layer 7	Private Crypto Key Management	Public Crypto Key Management Network Management Secure Message Handling Secure Directory Services
	Layer 4	SP4	
	Layer 3		SP3 (Connectionless) SP3 (Connection)
	Layer 2		Possibly IEEE 802.10
OSI Supporting Security Infrastructure		Security Labels Cryptographic Modules (DES) NIST Register for Uniquely Named Managed Security Objects	Trusted Functionality

"NIST Computer Security Object Register" (Presentation Slides), Lawrence Keys (NIST)

NIST Computer Security Object Register

Lawrence Keys, CSO Registrar

National Institute of Standards and Technology
Computer Systems Laboratory
Building 225, Room A216
Gaithersburg, Maryland 20899
(301) 975-5482

NIST Computer Security Object Register

Goals

* National/Federal Registration Authority
* Unique Name for Service Negotiation
* Catalogue for Users
* Information Distribution for Vendors

Status

* Draft Procedures for Registration
* NIST/CSL Support for Operation
* Request for Registration
* Seeking National Recognition/Approval

Registered Objects (Tentative Examples)

* Other Registration Authorities
* Cryptographic Algorithms
* Key Management Systems
* Security Domains
* Security Labels

Approach to Establishing CSO Register

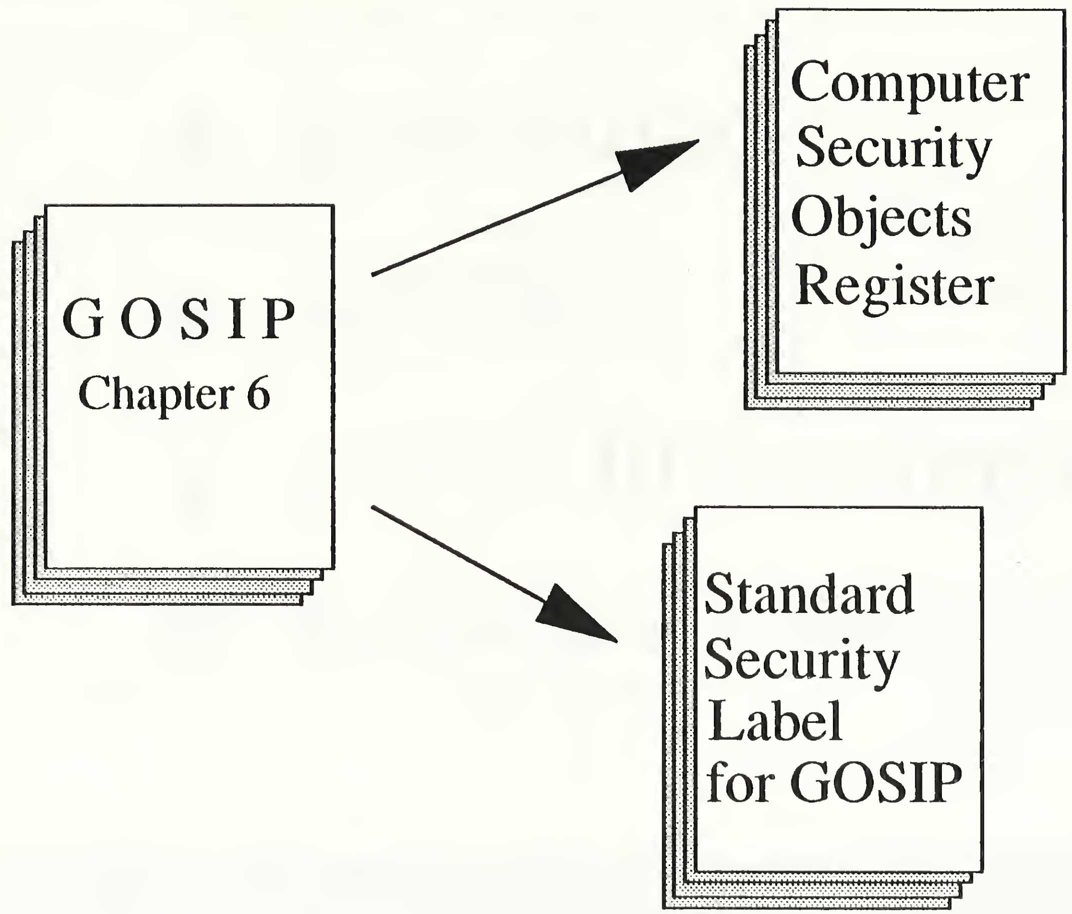
* **Federal Register notice of Intent to Develop Register**
* **Solicit comments on Registration Procedures**
* **Testing of Registration Procedures**
* **Publication of Final CSO Registration Procedures**

Proposed Procedures

* Applicant submits to NIST Request for Registration
    - Request must meet completness criteria for object
    - Registration fee must accompany registration
* NIST reviews request for completeness
* NIST searches Register for duplicate objects
* NIST shall assign a unique numeric value

"Standard Security Label for GOSIP" (Presentation Slides), Noel A. Nazario (NIST)

Standard Security Label for GOSIP



Standard Security Label for GOSIP

- Provides Label Syntax
- Layer Independent
- Flexible
- Extensible

Standard Security Label for GOSIP

- Format

Security Label Indicator C0 (hex)	Length Indicator	Security Information
1 OCTET	1 OCTET	

Register Index Code	Security Level	Security Tags
VAR	1 OCTET	VAR

Standard Security Label for GOSIP

- RIC

RIC Indicator	RIC Length Indicator	Index
1 OCTET	1 OCTET	VAR

  - RIC Indicator Value = CA (hex)
  - Index Values Assigned by CSOR

Standard Security Label for GOSIP

- Security Tag Type 0

00000000	00000000
Tag Type	Tag Length

- Security Tag Type 1

00000001	000LLLLL	CCCC CCCC
Tag Type	Tag Length	Bit Map

Standard Security Label for GOSIP

- Security Tag Type 2 (Set Inclusion)

00000010	000LLLLL	AAAA AAAA
Tag Type	Tag Length	Enumerated Attributes

- Security Tag Type 3 (Set Exclusion)

00000001	000LLLLL	AAAA AAAA
Tag Type	Tag Length	Enumerated Attributes

Standard Security Label for GOSIP

- Security Tag Type 4

00000100	000LLLLL	FFFF FFFF
Tag Type	Tag Length	Free Form Field

Standard Security Label for GOSIP

CLNP-IPSO vs SSL

- **CLNP-IPSO**
- Basic Option
  - Classification Protection Level
  - Protection Authority Flags
- Extended Option
  - Additional Information Format Code
  - Additional Security Information

- **SSL**
- A Single Option
  - Security Level
  - Register Index Code
  - Three Security Tag Types

Standard Security Label for GOSIP

CIPSO vs SSL

- **CIPSO**
  - Fixed Size DOI
  - One Level Field Per Tag

- **SSL**
  - Variable Size RIC
  - Single Security Level

Standard Security Label for GOSIP

What's Next

- Get Feedback
  - Editorial and Technical Comments
- Update Text
- Follow FIPS Approval Process

"Standard Security Label for the Government Open Systems Interconnection Profile" (Position Paper), Noel A. Nazario (NIST)

FIPS PUB xxx

Federal Information
Processing Standards Publication

Initial DRAFT 1991 February 28 *Initial DRAFT*

U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology

Standard Security Label for the Government Open Systems Interconnection Profile

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Robert Mosbacher, *Secretary*
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,
John W. Lyons, *Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235. These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal Government. The NIST, through the Computer Systems Laboratory, provides leadership , technical guidance, and coordination of Government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

James H. Burrows, Director
Computer Systems Laboratory

Abstract

This Standard specifies the format for a security label for the U.S. Government Open Systems Interconnection Profile (GOSIP). This network security label tells protocol processing entities how to handle unclassified but sensitive data communicated between open systems. Information carried by this label can be used to control access, specify protective measures, and indicate additional handling restrictions required by a network security policy.

Key words: ADP security, GOSIP security, network security labels, secure Open Systems Interconnection

Federal Information
Processing Standard Publication xxx

DRAFT 1991 February 28 *DRAFT*

ANNOUNCING A

Standard Security Label for the Government Open Systems Interconnection Profile

Federal Information Processing Standards are issued by the National Institute of Standards and Technology pursuant of the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Standard: Standard Security Label for Government Open Systems Interconnection Profiles.

Category of Standard: ADP Operations, Computer Security.

Explanation: This Standard specifies the format for a security Label within the U.S. Government Open Systems Interconnection Profile (GOSIP). Security labels indicate data sensitivity to accidental, unauthorized, intentional, or malicious disclosure, modification and destruction. Labels are used to control access, specify protective measures, and indicate handling restrictions required by a network security policy.

The label presented here contains a security level indicator and security tags that may carry compartments, caveats, and handling restrictions. Four security tag types provide for a bit map, two enumerated set representations (set inclusion and set exclusion), and a free form field.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Computer Systems Laboratory, National Institute of Standards and Technology.

Scope: This standard specifies a security label for GOSIP compliant implementations. The specified label may be used as a security feature at different layers of the Open Systems Interconnection (OSI) architecture. The specification given here is limited to the syntactic aspect of the label. The semantics of security labels, as defined for different security domains, are given by a Security Objects Register. Appendix B contains an example semantic definition for a label.

Applicability: The specified label applies to OSI network systems handling U.S. Government unclassified but sensitive data. This includes use by government agencies and commercial organizations conducting business with the Federal government.

Applications: The specified security label shall be used by OSI protocol processing entities to control access, specify protective measures and indicate handling restrictions required by a network security policy.

Implementations: Complying implementations shall be capable of transmitting, receiving, and handling the label format specified in this document.

Implementation Schedule: This standard becomes effective ...

Specifications: Federal Information Processing Standard (FIPS xxx) Standard for Information Security Labels (affixed).

Cross Index:

Waiver Procedure

Comments: Comments and questions may be addressed to:

Noel A. Nazario
National Institute of Standards and Technology
Bldg. 225 Rm A216
Gaithersburg, MD 20899

Where to Obtain Copies

Federal Information
Processing Standard Publication xxx

DRAFT 1991 February 28 *DRAFT*

Specifications for a

Standard Security Label for the Government Open Systems Interconnection Profile

1. INTRODUCTION

U.S. Government agencies are required to protect information assets essential to their operations. This includes both the protection of information within computer systems and while in transit over communications networks. This standard defines a network security label for use with the U.S. Government Open Systems Interconnection (OSI) Profile (GOSIP; FIPS PUB XXX).

The security label specified here can indicate data sensitivity to accidental, unauthorized, intentional, or malicious disclosure, modification and destruction. This label can also help to control access, specify protective measures, and indicate handling restrictions required by the network security policy.

2. REFERENCES

[1] European Computer Manufacturers Association, "Security in Open Systems - A Security Framework", ECMA TR/46, July 1988.

[2] European Computer Manufacturers Association, "Security in Open Systems - Data Elements and Service Definitions", ECMA Standard 138, December 1989.

[3] International Standards Organization (ISO), "Information processing systems - Open Systems Interconnection - Basic Model", ISO 7498, 1988.

[4] International Standards Organization (ISO), "Information processing systems - Open Systems Interconnection - Security Addendum", ISO 7498/2, 1988.

[5] Internet CIPSO Working Group, "Commercial IP Security Option", Proposed Request for Comments (RFC), February 7, 1991.

[6] Nazario Noel, "Security Labeling in Unclassified Networks", Proceedings of the 13th National Computer Security Conference, Volume 1, pp. 44-48, October 1990.

[7] "U.S. Government Open Systems Interconnection Profile" (GOSIP), FIPS PUB 146, August 1988.

3. DEFINITIONS AND ABBREVIATIONS

domain - See *security domain.*

GOSIP - (U.S.) Government Open Systems Interconnection Profile [7]

I - Index field

LI - Length Indicator

open system - A set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer which complies with the requirements of OSI standards in its communication with other open systems. [3]

OSI - Open System Interconnection [3]

PDU - Protocol data unit [3]

policy - See *security policy.*

RIC - Register Index Code

RIC-Ind - RIC Indicator

RIC-LI - RIC Length Indicator

security attribute - A security related quality of a security subject or security object. Security attributes may be represented as levels, compartments, caveats, et cetera.

security domain - A bounded group of security objects and security subjects to which applies a single security policy executed by a single security administrator. [1][2]

security label - Information that tells a protocol processing entity how to handle the data.

security object - Passive entity within a secure system (eg. secure file).

Security Objects Register - Set of security object definitions kept by a registration authority within a hierarchy.

security parameter - Property or quality identifying a piece of information. May indicate sensitivity to certain threat, degree of trust, access restrictions, classification, et cetera.

security policy - A set of rules which define and constrain the types of security relevant activities of entities.[2]

security threat - Circumstance with the potential to cause loss or harm to a computer system or the information it handles.

SI - Security Information

SL - Security Level

SLI - Security Label [Parameter] Indicator

TL - Additional Security Information Tag Length

TT - Additional Security Information Tag Type

4. SECURITY LABEL SPECIFICATION

4.1 General Format

This label format shall be used by Government Open Systems Interconnection Profile (GOSIP) implementations to provide security information to protocol processing entities. The format for the GOSIP security label is shown in figure 4.1.

This figure identifies three fields, Security Label Indicator, Length Indicator, and Security Information.

Security Label Indicator C0 (hex)	Length Indicator	Security Information
1 octet	1 octet	Var

Format Network Information Security Label
Fig. 4.1

4.2 Security Label Indicator

The size of the Security Label Indicator (SLI) field is 1 octet. The value of the SLI is 1100 0000 (C0 hex).

4.3 Length Indicator

The size of the Length Indicator (LI) field is 1 octet. This is the length of the Security Information Field. The value of the LI ranges between 8 and 128 octets.

4.4 Security Information

The variable length Security Information (SI) field contains the security label. This field is shown in Figure 4.2. The SI field contains the Register Index Code, a Security Level, and one or more Security Tags.

		Security Tag		
Register Index Code	Security Level	Additional Security Tag Type	Additional Security Tag Length	Additional Security Information
Var	1 octet	1 octet	1 octet	Var

Security Information Field
Fig. 4.2

4.4.1 Register Index Code

A Register Index Code (RIC) field points to the semantic definition of the label as registered in a Security Objects Register. The RIC is a variable size field. This field includes the RIC Indicator, RIC Length, and the Index field.

RIC Indicator	RIC Length Indicator	Index
1 octet	1 octet	Var

Register Index Code Field
Fig. 4.3

4.4.1.1 RIC Indicator

The size of the RIC Indicator (RIC-Ind) field is 1 octet. The binary value of this field is 1100 1010 (CA hex).

4.4.1.2 RIC Length Indicator

The size of the RIC Length Indicator (RIC-LI) field is 1 octet. Its value is the length of the Index (I) field in octets.

4.4.1.3 Index

The encoding of the index is given by the Security Objects Register. In the case when only part of an octet is required for encoding the index the significant bits will be left-justified and padded with 0.

4.4.2 Security Level

The size of the Security Level (SL) field is 1 octet, values range from 0 to 255. There is only one SL per label.

4.4.3 Security Tags

Additional security information is conveyed using Security Tags. A single label may have multiple variable size tags. Each Security Tag has fixed size type and length fields plus a variable size information field. The value of the length field in Tag Type 0 is zero; it contains no information.

4.4.3.1 Additional Security Tag Type

The size of the Additional Security Tag Type (TT) field is 1 octet. Its value indicates the tag type. Values range between 0 and 255. This standard defines tag types 0 through 4, all other tag types are reserved for definition by NIST's Security Objects Register. At least one tag must be present in every label.

4.4.3.2 Additional Security Tag Length

The size of the Additional Security Tag Length (TL) is 1 octet. The TL indicates the length of the information in the tag. Its value ranges between 0 and 30 octets. Note: This field is always zero for Tag Type 0.

4.4.3.3 Additional Security Information

This variable length field contains the value of the Security Tag. This document describes this field for Tag Types 1 - 4. Note: This field is not defined for Tag Type 0. All other tag types are reserved for definition by NIST's Security Objects Register.

4.4.3.3.1 Security Tag Type 0

Null tag, indicates end of the label. One (1) and only one (1) Tag Type 0 shall be present in any security label.

The format of tag 0 is as follows:

00000000	00000000
Tag Type	Tag Length

Security Tag Type 0
Fig. 4.4

4.4.3.3.2 Security Tag Type 1

The information carried by this tag is interpreted as a bit map of security attributes. The complete set of possible attributes is represented and those that apply are explicitly indicated. Length field values range between 1 and 30 octets.

In the bit map a bit N is set to 1 if attribute N (as defined in the register), is part of the label it is 0 if attribute N is not part of the label. Bits shall be numbered starting with the most significant bit of the first transmitted octet. Unused bits at the end the last octet are set to 0.

The format of this tag type is as follows:

00000001	000LLLLL	CCCC // CCCC
Tag Type	Tag Length	Bit Map

Security Tag Type 1
Fig. 4.5

4.4.3.3.3 Security Tag Type 2

Tag type 2 is used when only a few security attributes out of a large set apply to a protocol data unit (PDU). This is done by enumerating the attributes that apply (set inclusion). This enumeration shall start with the lowest numbered attribute following an ascending order. TL field values range between 2 and 30 octets.

A single tag may enumerate up to 15 security attributes, assigning 2 octets per attribute. The value for a security attribute may be between 0 and 65535.

The format of this tag type is as follows:

00000010	000LLLLL	AAAA // AAAA
Tag Type	Tag Length	Enumerated Attributes

Security Tag Type 2
Fig. 4.6

4.4.3.3.4 Security Tag Type 3

Tag type 3 is used when only a few security attributes out of a large set do not apply to a message. This is done by enumerating the attributes that do not apply to the PDU (set exclusion). Length field values range between 2 and 30 octets.

A single tag may enumerate up to 15 security attributes, assigning 2 octets per category. The value of each category can be from 0-65535.

The format of this tag type is as follows:

00000011	000LLLLL	AAAA // AAAA
Tag Type	Tag Length	Enumerated Attributes

Security Tag Type 3
Fig. 4.7

4.4.3.3.5 Security Tag Type 4

Tag type 4 carries a free format field of up to 30 octets. The information field of this tag may hold character strings, or any user-defined data. Length field values range between 1 and 30 octets.

The format of this tag type is as follows:

00000100	000LLLLL	FFFF // FFFF
Tag Type	Tag Length	Free Form Field

Security Tag Type 4
Fig. 4.8

4.5 Usage Rules

At most 1 security label may be used per layer PDU. The label described here shall be copied upon fragmentation. All multi-octet fields are defined to be transmitted in network byte order.

At least one tag must be present in every label. If no additional security information is required a NULL tag (Type 0) will be used. Only 1 NULL tag may appear in any label, it indicates the end of the label. The failure to find a NULL tag when expected and/or the finding of such tag when not expected are security relevant events that must be reported.

Multiple tags of types other than 0 may be present in a label. The detection of a label with information outside of the range permitted by the communicating parties must be reported as a security relevant event.

Appendix A

ASN.1 Definition for Standard Security Label

```
Standard Security Label ::= IMPLICIT  SEQUENCE {

      registerindexcode        RegisterIndexCode,

      securityLevel            OCTET STRING (SIZE(1)),

      securityTags             SEQUENCE OF SecurityTag OPTIONAL    }


RegisterIndexCode       ::= IMPLICIT  OCTET STRING


SecurityTag             ::= CHOICE  {

-- Type 0
      nulltag                          [0] IMPLICIT OCTET STRING (SIZE(0)),

-- Type 1
      bitMap                           [1] IMPLICIT OCTET STRING (SIZE(1..30)),

-- Type 2
      enumeratedAttributes             [2] IMPLICIT  SET OF SecurityAttribute,

-- Type 3
      complimentaryEnumAttributes      [3] IMPLICIT  SET OF  SecurityAttribute,

-- Type 4
      freeFormField                    [4] IMPLICIT  OCTET STRING (SIZE(1..30)) }


SecurityAttribute ::= IMPLICIT OCTET STRING (SIZE(2))
```

"CIPSO: Commercial Internet Protocol Security Option" (Presentation Slides), Ronald Sharp (AT&T)

CIPSO ORIGIN

- Based on work done by SUN and HP
- TSIG adopted the label with some modifications
- Currently in process to turn CIPSO specifications into an RFC

REASONS FOR CIPSO

1. RIPSO field values controlled by DCA

2. Security level limited to 8 values (only 4 defined)

3. Security level did not support commercial users or other governments

4. Security level and categories are in separate options

5. ESO was too undefined for vendors to developed generic implementation

CIPSO FEATURES

1. Supports multiple authorities for interpretation of field values
2. Well defined format for security labels
3. Can support other security label formats
4. Can support other security information (i.e. information labels)
5. Allows DOIs to specify format for tag types 129-255
6. DOI numbers to be administered by a recognized authority

CIPSO LABEL FORMAT

8 bits	8 bits	32 bits	8 bits	8 bits	? bits		8 bits	8 bits	? bits
134	6 - 40	1 - 0xffffffff	1-255	1-34	?	• • •	1-255	1-34	?
option number	option length	DOI	tag id	tag length	info field		tag id	tag length	info field

CIPSO TAG TYPE 1 FORMAT

8 bits	8 bits	8 bits	0 - 248 bits		
1	3 - 34	0 - 255	bit 1	• • •	bit 248
tag type	tag length	level	bit map of categories		

CIPSO TAG TYPE 2 FORMAT

8 bits	8 bits	8 bits	8 bits	16 bits		16 bits
2	4 - 34	0 - 255	0 - 255	cat 1	• • •	cat 15
tag type	tag length	level	flags	list of categories		

"Commercial IP Security Option" (Position Paper), Ronald Sharp (AT&T)

Internet CIPSO Working Group
Request for Comments: RFC XXXX
February 7, 1991

Commercial IP Security Option

1. Status of this Memo

This RFC proposes a Commercial IP Security Option (CIPSO) for the Internet community. This draft reflects the version as approved by the Internet CIPSO Working Group whose charter is to promote interoperability between vendors' trusted systems.

Distribution of this memo is unlimited.

2. Background

The Internet Protocol provides options for control functions that are useful in some situations but that are not necessary for the most common communications. One such option is the IP Security Option (Type 130) which allows IP packets to be labeled with security classifications, compartments, handling restrictions, and transmission control codes. This option provides sixteen security classifications. Compartments, handling restrictions and transmission control codes are all administered by the Defense Intelligence Agency (DIA) and Defense Communications Agency (DCA).

Recently a revision to the IP Security Option has been proposed in RFC 1038. This Revised IP Security Option (RIPSO) proposes a Basic Security Option (Type 130) and an Extended Security Option (Type 133). The Basic Security Option provides four security classifications and a set of protection authority flags that represent the accrediting authority(s) whose rules are to be followed in handling the datagram. The Extended Security Option provides additional security information as required by the registered authorities.

The term "Top Secret" is an example of a classification that is appropriate for the defense community. The term "Company Proprietary" is appropriate for commercial users. Words such as "accounting" and "personnel" are good examples of commercial compartments, whereas "nato" and crypto" are examples of compartments related to defense.

3. The Need for CIPSO

Computer vendors are now building commercial operating systems with mandatory access controls and multi-level security. These systems are no longer built specifically for a particular group in the defense or intelligence community. They are generally available commercial systems for use in a variety of environments.

The small number of RIPSO Authorities are not in a position to assign and register security related information for all the possible users of a commercial security option. Furthermore, users of such an option may not wish to have the details of their labeling policy known to others. (One such class of user, in particular, is other national governments.) Labeling policies may contain security classifications, compartments, and handling restrictions.

There are related efforts currently underway by various groups to define a session layer protocol to pass security information. It is important, however that security options that may be used for routing, continue to be passed at the IP layer. This allows routing decisions to be made based on security attributes. One such security attribute important for routing is the sensitivity label.

4. Current Internet Options

The following internet options are currently defined:

CLASS	NUMBER	LENGTH	DESCRIPTION
0	00000	-	End of Option list: This option occupies only 1 octet; it has no length octet.
0	00001	-	No Operation: This option occupies only 1 octet; it has no length octet.
0	00010	var.	Basic Security: Used to carry security level and accrediting authority flags.
0	00011	var.	Loose Source Routing: Used to route the datagram based on information supplied by the source.
0	00101	var.	Extended Security: Used to carry additional security information as required by registered authorities.
0	01001	var.	Strict Source Routing: Used to route the datagram based on information supplied by the source.
0	00111	var.	Record Route: Used to trace the route a datagram takes.
0	01000	4	Stream ID: Used to carry the stream identifier.
2	00100	var.	Internet Timestamp: Used to accumulate timing information in transit.

5. CIPSO

Option type: 134 (Class 0, Number 6, Copy on Fragmentation)
Option length: Variable

This option permits security related information to be passed between systems within a single Domain of Interpretation (DOI). A DOI is a collection of systems which agree on the meaning of particular values in the security option and which have a common security policy. A packet cannot have more than one CIPSO because it is not meaningful to apply more than one DOI to a packet.

This option must be copied on fragmentation. This option appears at most once in a datagram.

The format of this option is as follows:

```
+----------+---------+------//------+-----------//-----------+
|10000110 |000LLLLL | DDDDDDDDDDDD |  TTTTTTTTTTTTTTTTTTTT   |
+----------+---------+------//------+-----------//-----------+
 TYPE=134  OPTION    DOMAIN          TAGS
           LENGTH    OF
                     INTERPRETATION
```

FIGURE 1. CIPSO FORMAT

5.1 Type

This field is 1 octet in length. Its value is 134.

5.2 Length.

This field is 1 octet in length. It is the total length of the option including the type and length fields. Its values range from 6 to 40.

5.3 Domain of Interpretation

The length of this field is 4 octets. Its values are from 1-0xffffffff. The value 0 is reserved and must not appear in any CIPSO packet.

The DOI field provides the means for determining whether tags are known to a host (or IP router). It contains a value indicating the security domain within which the tags are to be interpreted.

Information concerning the registration of Domains of Interpretation may be obtained from [TBD].

5.4 Tag Types

A common format for passing security related information is necessary for interoperability. In CIPSO the security related information is defined to be a stream of tags that begin with a tag type identifier followed by the length of the tag. All multi-octet fields in a tag are defined to be transmitted in network byte order.

CIPSO tag types from 1 to 128 are defined by the Internet CIPSO Working Group. Tag types greater than 128 are user defined and may only be meaningful in certain Domains of Interpretation.

Tag type 0 is reserved. Tag types 1 and 2 are defined in this RFC. Types 3 and 4 are reserved for work in progress.

5.4.1 Tag Type 1

This is referred to as the "bit-mapped" tag type.

The format of this tag type is as follows:

```
+---------+---------+---------+--------//-----------+
|00000001 |000LLLLL |LLLLLLLL | CCCCCCCCCCCCCCCCC   |
+---------+---------+---------+--------//-----------+
 TAG       TAG       SECURITY  BIT MAP OF CATEGORIES
 TYPE      LENGTH    LEVEL
```

FIGURE 2. TAG TYPE 1 FORMAT

5.4.1.1 Tag Type

This field is 1 octet in length and has a value of 1.

5.4.1.2 Tag Length

This field is 1 octet in length. It is the total length of the tag type including the type and length fields. Its values are from 3 to 34.

If a host encounters a tag type it doesn't understand, it should be able to determine where the tag ends. It is possible for an unknown tag type to be followed by tag types that are understood by the host. A host's security policy may permit it to route partially understood packets (or it may be required to drop them).

5.4.1.3 Security Level

This field is 1 octet in length. Its values are from 0-255.

5.4.1.4 Bit Map of Categories

The length of this field is variable and ranges from 0 to 31 octets.

Bit N is 1 if category N (as defined for the DOI) is part of the label for the packet, and bit 0 if category N is not part of the label.

5.4.2 Tag Type 2

This is referred to as the "enumerated" tag type. It describes large but sparsely populated sets of categories.

The format of this tag type is as follows:

```
+---------+---------+---------+---------+---------//---------+
|00000010 |000LLLLL |LLLLLLLL |FFFFFFFF | CCCCCCCCCCCCCCCCC  |
+---------+---------+---------+---------+---------//---------+
 TAG       TAG       SECURITY  FLAGS     ENUMERATED
 TYPE      LENGTH    LEVEL               CATEGORIES
```

FIGURE 3. TAG TYPE 2 FORMAT

5.4.2.1 Tag Type

This field is one octet in length and has a value of 2.

5.4.2.2 Tag Length

This field is 1 octet in length. It is the total length of the tag type including the type and length fields. Its value is from 4 to 34 octets.

5.4.2.3 Security Level

This field is 1 octet in length. Its value is from 0-255.

5.4.2.4 Flags

This field is 1 octet in length.

The least significant bit of the flags field indicates whether the listed categories are included in or excluded from the enumerated tag type. If the exclusion flag is 0, the label represented by the enumerated tag contains all of the listed categories (from 0 to 15 of them). If the exclusion flag is 1, the label represented by the tag contains all categories defined by the DOI excluding the ones in the list. All other flag bits are unused.

5.4.2.5 Enumerated Categories

The length of each category is 2 octets. The value of each category can be from 0-65534.

Category 65535 is reserved and will not appear in any packet's CIPSO header.

6. Usage Rules.

The interpretation of the CIPSO is based on cooperating hosts within a security domain. The number and length of the tags are variable. Their total length can be computed from the option length.

If a packet is forwarded between different Domains of Interpretation, the forwarding IP router must translate between the interpretations. If such a translation would be incomplete or ambiguous, the packet must be discarded and an ICMP "parameter problem" (code 10) returned to the sender. (The packet header and the reason that it was discarded must be auditable.)

If the IP router has knowledge that the packet is out of range for the destination host or network, the packet must be discarded and an ICMP "destination unreachable" (code 3) returned to the sender. Perhaps a subcode should be defined to indicate "administrative restriction," or "label problem." (The packet header and the reason that it was discarded must be auditable.)

7. Restrictions

This option is not intended to replace either the IP Security Option, Basic Security Option, or Extended Security Option. Use of these options on a network where an accrediting authority exists is expected.

As defined, this option shouldn't stray onto networks where there isn't a Domain of Interpretation because it's easy to stop these packets in the IP router.

8. Other Considerations

8.1 The difference between CIPSO and RIPSO

RIPSO, as defined by RFC 1038, consists of two options: the Basic Security Option (BSO) and the Extended Security Option (ESO). The BSO contains the security level and some protection authority flags. The ESO provides a mechanism to include other security related information in the IP packet. Like CIPSO, it provides authorities that interpret the values for each field. Unlike CIPSO, there is no common format for the security label. The format is up to the associated authority. This will require a software change each time a new authority is added.

The primary difference between CIPSO and RIPSO is that the 8 possible authority codes in RIPSO are tightly controlled by DCA and the over 4 billion CIPSO authority (DOIs) codes are open to all commercial as well as Federal organizations. Other differences include the fact that RIPSO supports 8 security levels and CIPSO supports 256. In addition, RIPSO requires two options to send a security label and CIPSO requires only 1.

8.2 Size of the IP Option Field

The IP Options Field is limited to forty octets. With the size of today's inter-networks, source routing and record routing options can only provide limited end-to-end information. When combined with a security option(s) the situation becomes worse. It is possible for a single commercial security option which provides security classifications and compartments on a datagram to leave no room for routing information. This would make it difficult to debug routing decisions and impossible to specify a desired route. It may be time to consider provisions for a longer options field, such as a new revision of IP, or a flag bit indicating long options. (These two suggestions are probably equivalent from an inter-operability perspective.)

9. Acknowlegements

Much of the material in this RFC is based on (and copied from) work done by Gary Winiger of Sun Microsystems and published as *Commercial IP Security Option* at the INTEROP 89, Commercial IPSO Workshop.

10. Author's Address

Postal Address: < the Internet CIPSO Working Group point of contact>
Phone:
Email:

"GOSIP Security Chapter" (Presentation Slides), Noel A. Nazario (NIST)

GOSIP Security Chapter

GOSIP
Chapter 6

- Describes Security Options
- Placeholder for Future Specs
- New Paragraph Structure
- Points to SSL Doc and CSOR

CLNP Security Parameter

Octet	Bits 8765 4321	Field	
N	1100 0101	Parameter Code	
N+1	Len = B+E+1	Parameter Length	
N+2	XX00 0000	Security Format Code	Parameter Value
N+3 … N+B+2		Basic Information	
N+B+3 … N+B+E+2		Extended Information	
or			
N+3 … N+B+2		NIST Security Information	

- NIST Security Option
  - Format

Octets	Bits 8765 4321	
N	1000 1000	NIST Security Type Indicator
N+1	Len = I	Length of NIST Security Information
N+2 N+I+1		NIST Security Information

GOSIP Security Chapter

- NIST Security Option
  - NIST Security Information

    - Can hold several NIST-defined parameters
    - Only the Security Label Parameter is defined
    - Only one security label per PDU
    - Label Spec given in FIPS PUB XXX (SSL for GOSIP)
    - Semantics given by CSOR

"GOSIP Chapter 6 - Initial Draft for Version 3" (Position Paper), Noel A. Nazario (NIST)

G O S I P

Chapter 6

Initial Draft for Version 3

6. SECURITY OPTIONS

Security is of fundamental importance to the acceptance and use of open systems in the U.S. Government. Part 2 of the Open Systems Interconnection reference model (Security Architecture) is now an International Standard (IS 7498/2). The standard describes a general architecture for security in OSI, defines a set of security services that may be supported within the OSI model, and outlines a number of mechanisms than can be used in providing the services. However, no protocols, formats or minimum requirements are contained in the standard.

The text below describes security options that may be specified when incorporating security services to OSI Network and Transport Layers. This chapter does not describe at this time a complete set of security options that a user might desire nor a description of the security services and protocols that are associated with the specified parameters. Security labels are parameters that have been identified as needed if certain security services (e.g., confidentiality, access control) are incorporated to the OSI Layers. This chapter should be considered as a placeholder for future security specifications. Appendix 1 provides further information on what specifications are considered needed for OSI security.

As defined by ISO, security features are considered both implementation and usage options. An organization desiring security in a product that is being purchased in accordance with this profile must specify the security services required, the placement of the services within the OSI architecture, the mechanisms to provide the services and the management features required.

6.1 REASON FOR CLNP DISCARD PARAMETERS

The implementation of the security option requires assigning new parameter values to the Reason for Discard parameter in the CLNP Error Report PDU. The first octet of the parameter value contains an error type code as described in IS 8473. Values beyond those assigned in the standard are shown in Table 6.1. The second octet of the Reason for Discard parameter value either locates the error in the discarded PDU or contains the value zero as described in the standard.

Parameter Values		Class of Error	Meaning
Octet 1 Bits 8765 4321	Octet 2 Bits 8765 4321		
1101 0000	Discarded PDU Offset or Zero	Security	Security Option Out-of-Range
1101 1010	0000 0000	Security	Basic Portion Missing
1101 1101	0000 0000	Security	Extended Portion Missing
1101 0010	0000 0000	Security	Communication Administratively Prohibited

Table 6.1 Extended Values in the Reason For Discard Parameter

6.2 SECURITY PARAMETER FORMATS

6.2.1 OSI Application and Presentation Layer Security Parameter

To be determined

6.2.2 OSI Transport and Network Layer Security Parameter

IS 8473 defines the format of the Connectionless Network Protocol (CLNP) security parameter. This parameter consists of the three fields shown in Table 6.2. IS 8073, the Connection Oriented Transport Protocol Specification, leaves the definition of the security parameter to the user. The following specification shall be used by both protocols.

Octets	Bits 8765 4321	
N	1100 0101	Parameter Code
N + 1	Len = M	Parameter Length
N + 2 N + M + 1		Parameter Value

Table 6.2 Security Parameter Format

6.2.2.1 Parameter Code

IS 8473 assigns the value "1100 0101" to the Parameter Code field to identify the parameter as the Security Option.

6.2.2.2 Parameter Length

This octet indicates the length, in octets, of the Parameter Value field.

6.2.2.3 Parameter Value

The Parameter Value field contains the security information. IS 8473 defines only the first octet of the Parameter Value field. This section completes the definition of this field. Table 6.3 illustrates the format of the Parameter Value field within the Security Parameter.

	Bits 8765 4321		
N	1100 0101	Parameter Code	
N+1	Len = B+E+1	Parameter Length	
N+2	XX00 0000	Security Format Code	Parameter Value
N+3 N+B+2		Basic Information	
N+B+3 N+B+E+2		Extended Information	
or			
N+3 N+B+2		NIST Security Information	

Table 6.3 Format - Parameter Value Field

6.2.2.3.1 Security Format Code

As described in IS 8473, the high order two bits of the first octet of the Parameter Value field specify the Security Format Code. The standard reserves the remaining six bits and specifies that they must be zero.

The values of the Security Format Code are:

00	Reserved
01	Source Address Specific
10	Destination Address Specific
11	Globally Unique

6.2.2.3.2 Basic Security Option

The Basic Security Option of the Security Parameter identifies the U.S. Department of Defense classification level to which a PDU is to be protected and the authorities whose protection rules apply to that PDU. This option may appear at most once in a PDU. When the Basic Security Option appears in the Security Parameter of a PDU, it must be the first option in the Parameter Value field. This parameter may not be used together with the NIST Security Option. Section 6.2.3 defines the format of the Basic Security Option.

6.2.2.3.3 Extended Security Option

The Extended Security Option permits additional security labelling information beyond that present in the Basic Security Option. This extended information is supplied in a CLNP or Connection Oriented Transport PDU to meet the needs of registered authorities. This option may appear at most once in a PDU. The Extended Security Option must follow the Basic Option if it is present in the Security Parameter Value field. If an authority requires this option for a specific system, it must be specified explicitly in any Request for Proposal for that system. This parameter may not be used together with the NIST Security Option. Paragraph 6.2.4 defines the format of the Extended Option.

6.2.2.3.4 NIST Security Option

The National Institute of Standards and Technology (NIST) Security Option provides for a number of network security related parameters. The NIST Security Label is the only parameter type currently defined under this option. This parameter is specified in FIPS PUB XXX, Standard Security Label for the Government Open Systems Interconnection Profile. The NIST Security Label parameter provides a security level indicator and security information tags to convey security information on CLNP or Connection Oriented Transport PDUs. NIST reserves all other NIST Security Option parameter types. The security label parameter option may appear at most once in a PDU. This parameter may not be used together with the Basic and/or Extended Security Options. If this option is required by an authority for a specific system, it must be specified explicitly in any Request for Proposal for that system. Paragraph 6.2.5 defines the format of the NIST Security Option.

6.2.3 BASIC SECURITY OPTION

The Basic Security Option is used by the components of an internetwork to:

A. Transmit from source to destination, in a network standard representation, the common DoD security labels.

B. Validate the PDU as appropriate for transmission from the source and delivery to the destination.

C. Ensure that the route taken by the PDU is protected to the level required by all protection authorities indicated on the PDU.

Table 6.4 shows the format of the Basic Security Option.

Octets	Bits 8765 4321	
N	1000 0010	Basic Type Indicator
N+1	Len = I	Length of Basic Information
N+2 N+I+1		Basic Information

Table 6.4 Format - Basic Security Option

6.2.3.1 Basic Type Indicator

The value of this field identifies this as the Basic Security Option.

6.2.3.2 Length of Basic Information

This length field, when present, indicates the length, in octets, of the Basic Information field. The Basic Information field is variable in length and has a minimum length of two octets.

6.2.3.3 Basic Information

The Basic Information field consists of two subfields as Table 6.5 illustrates.

Octets	Bits 8765 4321		
B	1000 0010	Basic Type Indicator	
B + 1	Len = F + 1	Length of Basic Information (Minimum = 2 Octets)	
B + 2		Classification Level	Basic Information
B + 3 B + F + 2		Protection Authority Flags	

Table 6.5 Format - Basic Information Field

6.2.3.3.1 Classification Level

The Classification Level field specifies the U.S. DoD classification level to which the PDU must be protected. The information in the PDU must be treated at this level unless it is regraded in accordance under the procedures of all the authorities identified by the Protection Authority Flags. The field is one octet in length. Table 6.6 provides the encodings for this field.

VALUE Bits 8765 4321	LEVEL
0000 0001	RESERVED 4
0011 1101	TOP SECRET
0101 1010	SECRET
1001 0110	CONFIDENTIAL
0110 0110	RESERVED 3
1100 1100	RESERVED 2
1010 1011	UNCLASSIFIED
1111 0001	RESERVED 1

Table 6.6 Classification Levels

6.2.3.3.2 Protection Authority Flags

The Protection Authority Flags field indicates the National Access Program(s) or Special Access Program(s) whose rules apply to the protection of the PDU. Its field length and source flags are described below. To maintain the architectural consistency and interoperability of DoD common user data networks, users of these networks should submit requirements for additional Protection Authority Flags to DCA DISDB, Washington, D. C. 20305-2000 for review and approval.

A. Field Length: The Protection Authority Flags field is variable in length. The low order bit (Bit 1) of an octet is encoded as "0" if the octet is the final octet in the field. If there are additional octets, then the low order bit is encoded as "1". Currently, there are less than eight authorities. Therefore, only one octet is required and the low order bit of this octet is encoded as "0".

B. Source Flags: Bits 2 through 8 in each octet are flags. Each flag is associated with an authority as indicated in Table 6.7. The bit corresponding to an authority is "1" if the PDU is to be protected in accordance with the rules of that authority.

Bit Number	Authority	Point of Contact
8	GENSER	Designated Approving Authority per DoD 5200.28
7	SIOP-ESI	Department of Defense Organization of the Joint Chiefs of Staff Attn: J6T Washington, D.C.
6	SCI	Director of Central Intelligence Attn: Chairman, Information Handling Committee Intelligence Community Staff Washington, D. C. 20505
5	NSA	National Security Agency 9800 Savage Road Attn: T03 Ft. Meade, MD 20755-6000
4	DOE	Department of Energy Attn: DP343.2 Washington, D.C. 20545
3 , 2	Unassigned	
1	Extension Bit	Presently always "0"

Table 6.7 Protection Authority Bit Assignments

6.2.4 EXTENDED SECURITY OPTION

Table 6.8 illustrates the format for the Extended Security Option. To maintain the architectural consistency of DoD common user data networks, and to maximize interoperability, users of these networks should submit their plans for the use of the Extended Security Option to DCA DISDB, Washington, D.C. 20305-2000 for review and approval. Once approved, DCA DISDB will assign Additional Security Information Format Codes to the requesting activities.

Octets	Bits 8765 4321	
N	1000 0101	Extended Type Indicator
N+1	Len = I	Length of Extended Information
N+2 N+I+1		Extended Information

Table 6.8 Format - Extended Security Option

6.2.4.1 Extended Type Indicator

The value of this field identifies this as the Extended Security Option.

6.2.4.2 Length of Extended Information

This length field indicates the length, in octets, of the Extended Information field. The Extended Information field is variable in length with a minimum length of two octets.

6.2.4.3 Extended Information

The Extended Information field consists of three subfields as Table 6.9 illustrates. These three fields form a sequence. This sequence may appear multiple times, forming a set, within the Extended Information field.

	Octets	Bits 8765 4321		
	E	1000 0101	Extended Type Indicator	
	E+1	Len = (B - A) + 1	Length of Extended Information (Minimum = 2 Octets)	
A	E+2		Additional Security Information Format Code	
	E+3	Len = I	Length of Additional Security Information	
	E+4 E+I+3		Additional Security Information (Zero or more octets)	
		(Additional Sequences of the above three fields)		Extended Information
	E+N		Additional Security Information Format Code	
	E+N+1	Len = J	Length of Additional Security Information	
B	E+N+2 E+N+J+1		Additional Security Information (Zero or more octets)	

Table 6.9 Format - Extended Information Field

6.2.4.3.1 Additional Security Information Format Code

The value of the Additional Security Information Format Code corresponds to a particular format and meaning for a specific Additional Security Information field. Each format code is assigned to a specific controlling activity. Once assigned, this activity becomes the authority for the definition of the remainder of the Additional Security Information identified by that format code. A single controlling activity may be responsible for multiple format codes. However, a particular format code may appear at most once in a PDU. For each Additional Security Information Format Code an authority is responsible for, that authority will provide sufficient criteria for determining whether a CLNP PDU marked with its Format Code should be accepted or rejected. Whenever possible, this criteria will be Unclassified.

Note: The bit assignments for the Protection Authority flags of the Basic Security Option of the Security Parameter have no relationship to the "Additional Security Information Format Code" of this option.

6.2.4.3.2 Length of Additional Security Information

This field provides the length, in octets, of the "Additional Security Information" field immediately following.

6.2.4.3.3 Additional Security Information

The Additional Security Information field contains the additional security relevant information specified by the authority identified by the "Additional Security Information Format Code." The format, length, content, and semantics of this field are determined by that authority. The minimum length of this field is zero.

6.2.5 NIST SECURITY OPTION

Table 6.10 illustrates the format for the NIST Security Option. To maintain the architectural consistency of common user data networks, and to maximize interoperability, users of these networks shall submit their plans for the use of the NIST Security Option to Registrar, Security Objects Register, National Institute of Standards and Technology, Bldg. 225 Rm. A216, Gaithersburg, MD 20899 for review and approval.

Bits 8765 4321		
Octets N	1000 1000	NIST Security Type Indicator
N+1	Len = I	Length of NIST Security Information
N+2 N+I+1		NIST Security Information

Table 6.10 Format - NIST Security Option

6.2.5.1 NIST Security Type Indicator

The value of this field identifies this as the NIST Security Option.

6.2.5.2 Length of NIST Security Information

This length field indicates the length, in octets, of the NIST Security Information field. The NIST Security Information field is variable in length with a minimum length of two octets.

6.2.5.3 NIST Security Information

The NIST Security Information can hold several NIST defined parameters. Only one parameter, the NIST Security Label, is currently defined. The specification for this label is given in FIPS PUB XXX, Standard Security Label for the Government Open Systems Interconnection Profile. Only one security label may be present in the NIST Security Information parameter field. The semantic rules for the usage and interpretation of the NIST Security Label are given by the NIST Security Objects Register.

6.2.6 Usage Guidelines for the Basic and Extended Security Options

A PDU is "within the range" if

MIN-LEVEL <= PDU-LEVEL <= MAX-LEVEL

where MIN-LEVEL and MAX-LEVEL are the minimum and maximum security levels, respectively, that the system is accredited for. The term PDU-LEVEL refers to the security level of the PDU. In this context, the "security level" may involve the combination of three factors:

1) classification level
2) protection authorities
3) additional security labelling information as required and defined by the responsible activity.

The authorities responsible for accrediting a system or collection of systems are also responsible for determining whether and how these factors interact to form a security level or security range. A PDU should be accepted for further processing only if it is within range. Otherwise, the Out-of-Range procedure described in Paragraph 6.6 should be followed.

6.2.6.1 Basic Security Option

Use of the information contained in the Basic Security Option requires that an end system be aware of:

A. the classification level, or levels, at which it is permitted to operate, and

B. the protection authorities responsible for its accreditation.

Representation of this configuration information is implementation dependent.

6.2.6.2 Extended Security Option

Use of the Extended Security Option requires that the end system configuration accurately reflects the accredited security parameters associated with communication via each network interface. Representation of the security parameters and their binding to specific network interfaces is implementation dependent.

6.2.7 Out-of-Range Procedure for PDU's protected by the Basic and Extended Security Options.

If the Out-Of-Range condition was triggered by:

A. A required, but missing, Security Option or Basic or Extended Security Option, then the PDU should be discarded. In addition, a CLNP Error Report or other form of reply is not permitted in this case. However, a local security policy may permit data to be delivered or a CLNP Error Report PDU to be processed provided a reply is not sent.

B. A PDU whose security level is less than the end system's minimum security level, then the PDU should be discarded. In addition, a CLNP Error Report or other form of reply is not permitted in this case. However, local security policy may permit data to be delivered or a CLNP Error Report PDU to be processed provided a reply is not sent.

C. A PDU whose security level is greater than the end system's maximum security level, then:

1. If a CLNP Error Report PDU triggered the Out-of-Range condition, then no reply is permitted and the PDU should be discarded. A CLNP Error Report PDU must not be sent in this case.

2. Otherwise, discard the PDU and send a CLNP Error Report PDU to the originating CLNP entity. The first octet of the Reason for Discard parameter is set as specified in Table 6.1. The second octet of the Reason for Discard parameter identifies the Out-of-Range Security Option. It should point to the first octet (i.e., the type indicator) of the Out-of-Range option. Alternatively, the second octet can be set to zero. The response is sent at the maximum classification level of the end system which received the PDU. The protection authority flags are set to be the intersection of those for which the host is accredited and those present in the PDU which triggered this response.

Example: PDU = "Secret, GENSER"
End System Level = "Unclassified, GENSER".
Reply = "Unclassified, GENSER".

These are the least restrictive actions permitted by this protocol. Individual end systems, system administrators, or protection authorities may impose more stringent restrictions on responses and in some instances may not permit any response at all to a PDU which is outside the accredited security range of an end system.

6.2.8 Trusted Intermediary Procedure for communications protected by the Basic and Extended Security Options.

Certain devices in an internetwork may act as intermediaries to validate that communications between two end systems is authorized. This decision is based on a combination of knowledge of the end systems and the values in the CLNP Security Option. [The Blacker Front End (BFE) is one example of such a trusted device.] These devices may receive CLNP PDUs which are in range for the intermediate device, but are either not within the accredited range for the source or the destination. In the former case, the PDU should be treated as described in Paragraph 6.6. In the latter case, a CLNP Error Report PDU should be sent to the originating CLNP entity. The first octet of the Reason for Discard parameter should be set to 1101 0010. This code indicates to the originating CLNP entity that communication with the end system is administratively prohibited (refer to Table 6.1). The security range of the interface on which the reply will be sent determines whether a reply is allowed and at what security level it should be sent.

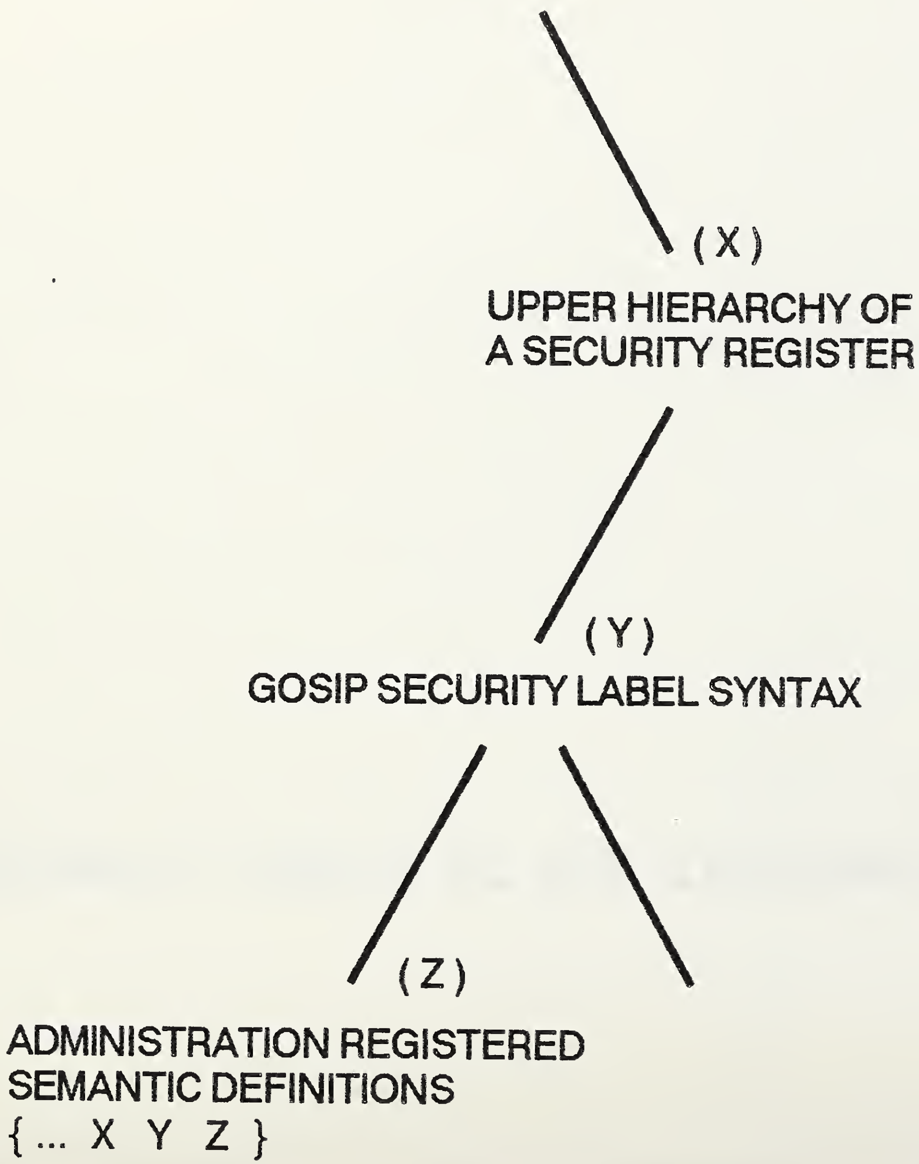
"Security Labels at the Transport Layer" (Presentation Slides), Wayne A. Jansen (NIST)

SECURITY LABELS AT THE TRANSPORT LAYER

W.A. JANSEN
NIST, CSL
4/1/91

C0.06 .CA.01.DC.99.00.00

REGISTRATION OF LABEL SYNTAX AND SEMANTICS



GOSIP SECURITY LABEL

DRAFT STANDARD SECURITY LABEL FOR GOSIP

C0 HEX	LENGTH	RIC TYPE INDICATOR	LENGTH OF RIC	REGISTER INDEX
1	1	1	1	VAR

DETERMINES HOW THE REMAINDER OF THE LABEL IS INTERPRETED

THE REMAINDER OF THE LABEL

SECURITY LEVEL	SEQUENCE OF OPTIONAL SECURITY TAGS	NULL TAG
1	VAR	2

TRANSPORT LAYER SECURITY LABELS

CD OSI TRANSPORT LAYER SECURITY PROTOCOL

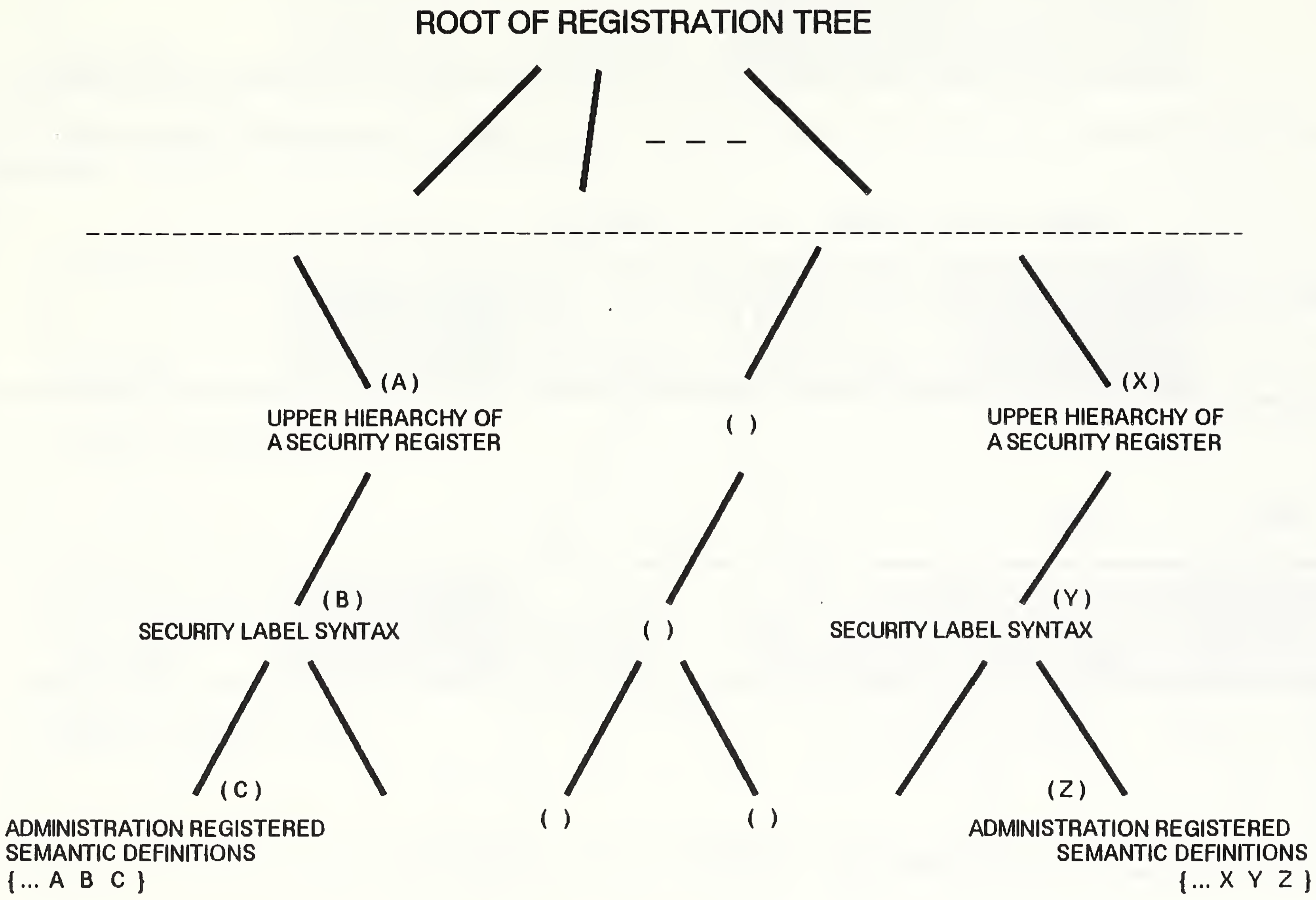
C0 HEX	LENGTH	DEFINING AUTHORITY	VALUE
1	1	1	VAR

US BALLOT RESPONSE PROPOSED CHANGE

C0 HEX	LENGTH OF DEFINING AUTHORITY	DEFINING AUTHORITY	LENGTH OF VALUE	VALUE
1	1	VAR	1	VAR

DETERMINES HOW THE VALUE FIELD
IS ENCODED AND INTERPRETED

TRANSPORT VIEW OF LABEL REGISTRATION



ALIGNMENT OF LABEL FORMATS

DRAFT GOSIP LABEL

C0 HEX	LENGTH	~~RIC TYPE INDICATOR~~	LENGTH OF RIC	REGISTER INDEX	
1	1	~~1~~	1	VAR	VAR

LABEL ALIGNMENT

C0 HEX	LENGTH	LENGTH OF RIC	REGISTER INDEX	REGISTERED ENCODING
1	1	VAR	VAR	VAR

PROPOSED TRANSPORT LABEL

C0 HEX	LENGTH OF DEFINING AUTHORITY	DEFINING AUTHORITY	LENGTH OF VALUE	VALUE
1	1	VAR	1	VAR

AN ABSTRACT LABEL FORMAT DEFINITION

ABSTRACT SYNTAX NOTATION.1

```
Security – Label ::= IMPLICIT SEQUENCE {
        administration – registration – index   OBJECT IDENTIFIER,
        security – information   ANY DEFINED BY administration – registration – index
        }
```

PRESENTATION LAYER
BASIC ENCODING RULES

SECURITY LABEL	T L V
ARI	T L V
SI	T L V

TRANSPORT/NETWORK LAYER
ENCODING RULES

SECURITY LABEL	T L V
ARI	L V
SI	. . .

SECURITY LABELS AT THE TRANSPORT LAYER

SUMMARY

- A COMMON CONCRETE SYNTAX DEFINITION OF THE GOSIP SECURITY LABEL FOR BOTH THE NETWORK AND TRANSPORT LAYERS IS POSSIBLE
- AN ASN.1 DEFINITION OF THE GOSIP SECURITY LABEL FORMS A GOOD STARTING POINT FOR DERIVATION OF A CONCRETE SYNTAX DEFINITION
- EFFICIENT ENCODING RULES APPROPRIATE FOR REPRESENTING GOSIP SECURITY LABELS AT THE LOWER LAYERS CAN BE DETERMINED
- AN INDEFINITE LENGTH ENCODING OF THE REGISTRATION INDEX MAY BE NEEDED FOR GENERAL APPLICATION

Comments on the draft FIPS - "Standard Security Label for the Government Open Systems Interconnection Profile" (Position Paper), Russell Housley, Sammy Migues (Xerox Special Information Systems)

Comments on the draft FIPS

Standard Security Label for the Government Open Systems Interconnection Profile

Russell Housley
Sammy Migues
Xerox Special Information Systems
7900 Westpark Drive, Suite A210
McLean, VA 22102

1.0 Introduction

We thank NIST for the opportunity to comment on this document. We found it to be well-written and representative of a great deal of work.

2.0 Overall Comments

The draft FIPS defines a label that is appropriate for use within CLNP. Perhaps, it is also applicable to other protocols such as TP, SP3, and SP4 (but this is not stated). However, it is not appropriate for application layer protocols and such a label should be defined using ASN.1. There is some ongoing standards work in IEEE 802.2 to define a LAN security label and this document should definitely be used to influence their work.

We feel that security label definitions are needed for layers two, three, four, and seven. A label is needed in layer two so that bridges can make relay decisions. A label is needed in layer three so that routers can make routing decisions. A label is needed in layer four to support trusted multiplexing and demultiplexing. Layer four could also be used to label end system to end system data transfers. Layer seven labels are needed for end system to end system data transfers where only the application knows enough about what is going on to be able to label the data appropriately.

3.0 Specific Comments

Abstract: Is the use of "network security label" meant to imply the use of the network layer? Also, is there a reason why "secure" Open Systems Interconnection was chosen versus "trusted" Open Systems Interconnection? "Secure" also occurs twice in the definition of security object.

Announcement Page, Explanation Section: The sentence "Security labels indicate data sensitivity to ..." might be rewritten as "Security labels indicate the degree of potential loss due to..." The actual classification of the data does necessarily make it more sensitive (as in "is easier to") to destruction or modification. This sentence also occurs on Page 1.

Announcement Page, Applicability Section: There appears to be a missing or misspelled word in "This includes use government agencies..."

Page 2: In the definition of "security object," what is a "secure file"?

Page 2: In the definition of "security parameter," how does a security parameter "identify" a piece of information?

Page 5, Figure 4.3: Why is the RIC Indicator necessary since the RIC is always the first field of security information and the RIC must always be present?

Page 5, Section 4.4.1.3: This is an ambiguous encoding method. If the significant bits are left-justified and padded with zeros, then the values 1, 2, 4, 8, etc., will all have the same encoding.

Page 6, Section 4.4.3: It should be stated here that at least one security tag must be present in each security label.

Page 6, Section 4.4.3.2: Does the tag length really reveal the length of the tag or does it only reveal the length of the tag additional security information?

Page 6, Section 4.4.3.3: Should the phrase "is not defined" be "is of zero length"?

Page 7, Section 4.4.3.3.2: The second sentence of the first paragraph must be given more punctuation or rewritten.

Page 8, Section 4.4.3.3.4: In the first sentence of the first paragraph, the last word should be "PDU" instead of "message". In the second paragraph, the word "attributes" should be substituted for the word "category" in both places.

4.0 Conclusions

Here are our general conclusions on this draft FIPS:

1. The draft FIPS should specifically state the protocols to which it applies.

2. The draft FIPS should state that the security label applies only to the data in the PDU and that it does not apply to the protocol control information or to itself.

3. We recommend that a layer seven label be defined using ASN.1.

4. We recommend interaction with IEEE 802.2 on the definition of a LAN security label.

"The Multipolicy Machine - A New Paradigm for Multilevel Security Systems" (Position Paper), Hilary Hosmer (Data Security, Inc.

THE MULTIPOLICY MACHINE

A NEW PARADIGM FOR MULTILEVEL SECURE SYSTEMS

HILARY HOSMER
DATA SECURITY INC
58 Wilson Road
Bedford, MA 01730

ABSTRACT

The Multipolicy Machine is a paradigm shift in multilevel secure (MLS) computer architecture. It permits an MLS system to enforce multiple, perhaps contradictory security policies. Multiple policies permit more natural modelling of real-world security practices and allow easier sharing of data among users in different security domains.

The multilevel secure system of today enforces a single system security policy, causing integration problems when products with slightly different policies (OS, DBMS, user applications) must work together. The single system policy also makes it difficult for two systems enforcing different policies (NATO, US, for example) to share data.

In the Multipolicy Machine concept, each MLS computer node is capable of enforcing a variety of security policies, and data carries policy domain codes to indicate which security policies apply. Metapolicies coordinate the interactions of security policies. Thus data can be transferred from one node to another and still be protected by the appropriate security policies.

Military applications include C3 systems in multinational and multiservice battle theaters. Commercial applications include medical, financial, and investigative systems that cross policy domains.

INTRODUCTION

This paper identifies fundamental problems with the current trusted system paradigm, describes requirements for a new paradigm, and proposes a new multipolicy paradigm. The recommended change is analogous to moving a country from a monarchy to a democracy.

The paper presents several alternative strategies for a building a Multipolicy Machine. It explores the critical metapolicy concept and raises issues about technical feasibility, control, NCSC acceptance, evaluation and export.

The Multipolicy Machine is being presented at the NIST Labels Workshop to encourage discussion about the current security paradigm and to make sure that the proposed GOSIP label standard is flexible enough to permit multipolicy computer security architectures.

BACKGROUND

The Trusted Computer System Evaluation Criteria (TCSEC or Orange Book) defines the United States' security paradigm. It assumes a single 'system security policy' which is divided into three major subpolicies: Confidentiality, Integrity, and Assurance of Service. The subpolicies are further subdivided. Confidentiality is divided into Access Control and Non-Access Control policies. Access Control policies are subdivided into Mandatory Access Control (MAC) and Discretionary Access Control (DAC). However, the paradigm assumes that all these subpolicies cohere together to represent one overall system security policy. The single overall policy drives the choice of security mechanisms and is the foundation of most assurance efforts.

The single-policy paradigm works well with stand-alone systems but causes problems when security policy integration is required. For example, when MLS products each with a slightly different policy such as Operating System (OS), Database Management System (DBMS), and user applications must interoperate as one system, there may be integration difficulties[1]. Similarly, when systems enforcing different policies, such as U.S.A. Department of Defense (DOD), North Atlantic Treaty Organization (NATO), European Community (EC), and France, must interact and share classified data compromises must be made. For several years, computer security founder Dr. Willis Ware has called for a new

[1] Hosmer, Hilary H. "Integrating Security Policies", <u>Proceedings of the Third RADC Workshop of Multilevel Database Security</u>, Castile, NY, June 1990.

paradigm which will make networking and integration of MLS systems easier.

This paper proposes such a paradigm.

PROBLEMS WITH THE CURRENT PARADIGM

The single-policy paradigm has some major flaws which are becoming apparent now that multilevel secure systems are being fielded.

> *It's inflexible.* If a user wants to modify the system security policy, the whole system must be reevaluated.
>
> *Exchanging data with systems with other security policies is difficult or impossible in real-time.* Guards are needed at all interfaces, and mapping rarely can translate security levels from one policy to the other without upgrading.
>
> *Its unrealistic.* The real world has multiple coexistent security policies. Users must integrate diverse and contradictory policies together into a single coherent policy.
>
> *Performance is poor.* Adding security to existing systems seriously slows down throughput.

The current paradigm must be enlarged to meet the needs of a more interrelated and integrated world. With a few significant enhancements, the single-policy paradigm can be extended into a more flexible, more interoperative, better-performing multipolicy paradigm.

REQUIREMENTS

What must a larger and more inclusive paradigm do? It should:

Handle bottom-up system construction. The end-user, supposedly the originator of the system security policy, can't change the security policy already implemented without reevaluation. The end-user must purchase components with security policies that come close to his needs, but a perfect match is unlikely. We need a paradigm which permits the end-user to establish his own security policy in a near-match system without requiring a reevaluation of the whole system.

Separate policy from policy enforcement mechanisms. Because of the single-policy paradigm, current trusted systems implement the system security policy as an integral part of the system. It is often impossible to separate the policy from the mechanisms which implement that policy. A more flexible paradigm would separate policy from mechanism so that mechanisms can enforce more than one policy, and policies can be tailored.

Ease integration of trusted system components. Under the single-policy paradigm, each purchased component, including hardware, operating system, DBMS, and applications packages, must be integrated into a coherent package that can be proven to implement the end-user's security policy. This integration is difficult when diverse vendors' components implement slightly different security policies or slightly different versions of the same security policy. We need a paradigm which has standards or one which accommodates policy variations.

Ease sharing data with other policy systems. The 'single system security policy' founders on the pressing need to share data with allies, military or commercial, who have different security policies. In multinational conflicts such as that of the Persian Gulf, users of a computer system with a US DoD security policy need to share data with other computers that implement different national or international security policies. Current strategies for sharing data across security policy boundaries (Guards, Man-in-the-loop) frequently must upgrade or downgrade data, thus losing the original classification. The assessment time required for down-grading makes it difficult to share data in real-time in a fast-moving multinational battlefield situation. Even if the multinational situation is one of cooperation rather than conflict (for example, divisions of a multinational corporation, or international electronic funds transfer), we would like to be able to enforce the originator's security policy while sharing data among computer systems.

Permit contradictory policies to operate in parallel. The current definition may preclude systems such as a national AIDS databank which enforces many different Mandatory Access Control (MAC) policies (one for each state, plus one for the nation) to apply the varying state regulations on the release of AIDS data. It makes it difficult to build the European Community health system where the varying disclosure laws of 12 different countries must be implemented. A new paradigm which permits contradictory policies to operate in parallel is needed.

Improve the performance of trusted systems.

Other. The list above is not exhaustive. As more multilevel systems are implemented, we will become aware of more difficulties and requirements.

Solving these problems is essential to widespread user acceptance of MLS systems.

THE OPPORTUNITY OF THE MULTIPOLICY MACHINE

A Multipolicy Machine will solve significant portions of these long-standing problems. First, it provides a vehicle for users to add their own security policies to a system without disrupting or invalidating existing evaluated policies. Secondly, it eases integration problems by preserving the original classification of data when data is passed across policy boundaries. Thirdly, it permits one machine to enforce a variety of parallel security policies which are not necessarily consistent with one another. Fourthly, it may improve trusted system performance by being implemented in high-speed parallel processing architecture.

There are several key questions. First, how do you build a Multipolicy Machine? Secondly, how do you prove that it's secure? Thirdly, will the security community accept it? Fourthly, is it cost-effective?

BUILDING THE MULTIPOLICY MACHINE

Components

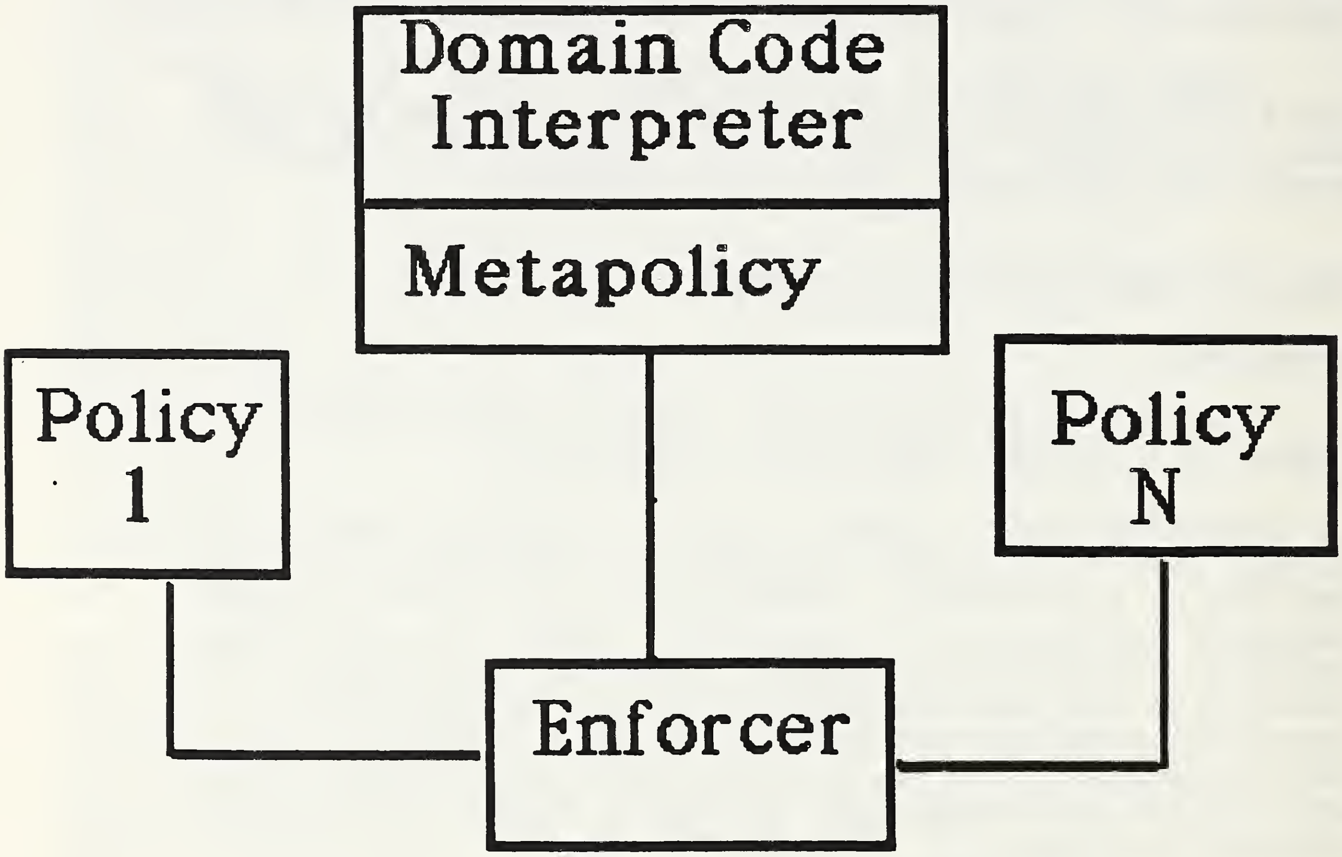
A multipolicy machine has three elements which do not appear in current single-policy products:

1. *Security policy domain codes on security labels*. Every object must have a code indicating which security policy applies to this object. This is similar to the European Computer Manufacturers Association (ECMA) security domain codes on security labels which indicate under which label convention the label is formatted, eg. International Standards Organization (ISO)). If more than one security policy applies, such as a DoD policy, an Air Force Policy, and a local Air Force Base policy, a policy domain code is required for each.

Object	Security Label	Policy Domain Codes

2. *Domain code interpreters.* A security domain code interpreter will check the domain codes and direct the label to the proper security policy enforcers.

3. *Metapolicies.* A key to successful implementation of any of these approaches is a successful coordinator of security policies. When one piece of data is labeled with three security policies, such as DoD, Air Force, and Hanscom AFB, there must be rules about which policy to apply first, which second, and which third. When one policy contradicts a second policy, there must be instructions for handling these discrepancies. For example, if one state prohibits release of certain AIDS data while another state requires the same data be reported to authorities, what should be done if a patient from the first state is hospitalized in the second state? In addition, there should be a provision for authorized and audited metapolicy override. A later section will look at metapolicy issues more closely.



A multipolicy machine also has multiple versions of security elements which are standard in all single-policy systems. These include security policies and security policy enforcers.

As in a single policy machine, security policies consist of: a) definitions of subjects and objects; b) definitions of allowable operations; and c) the rules of the policy, including a policy lattice for ordering sensitivity levels, integrity levels, compartments, et cetera. As in the single-policy machine, each policy is separate from the others and tamperproof. However, each computer may have more than one policy. If appropriate, a computer could have a copy of every policy implemented in the network.

Security policy enforcers implement the rules of a policy on the subjects and objects. A Reference Monitor is an example of an access control policy enforcer. Each enforcer is trusted to protect and enforce policies correctly, and must be tamperproof.

Implementation Options

There are several reasonable approaches to the implementation of a multipolicy machine.

1. Multiple sets of rule-based policies;
2. Multiple co-processors;
3. Distributed policies;
4. Parallel processors;
5. Redundant fault-tolerant policies.

Each option is described briefly below.

Rule-based.

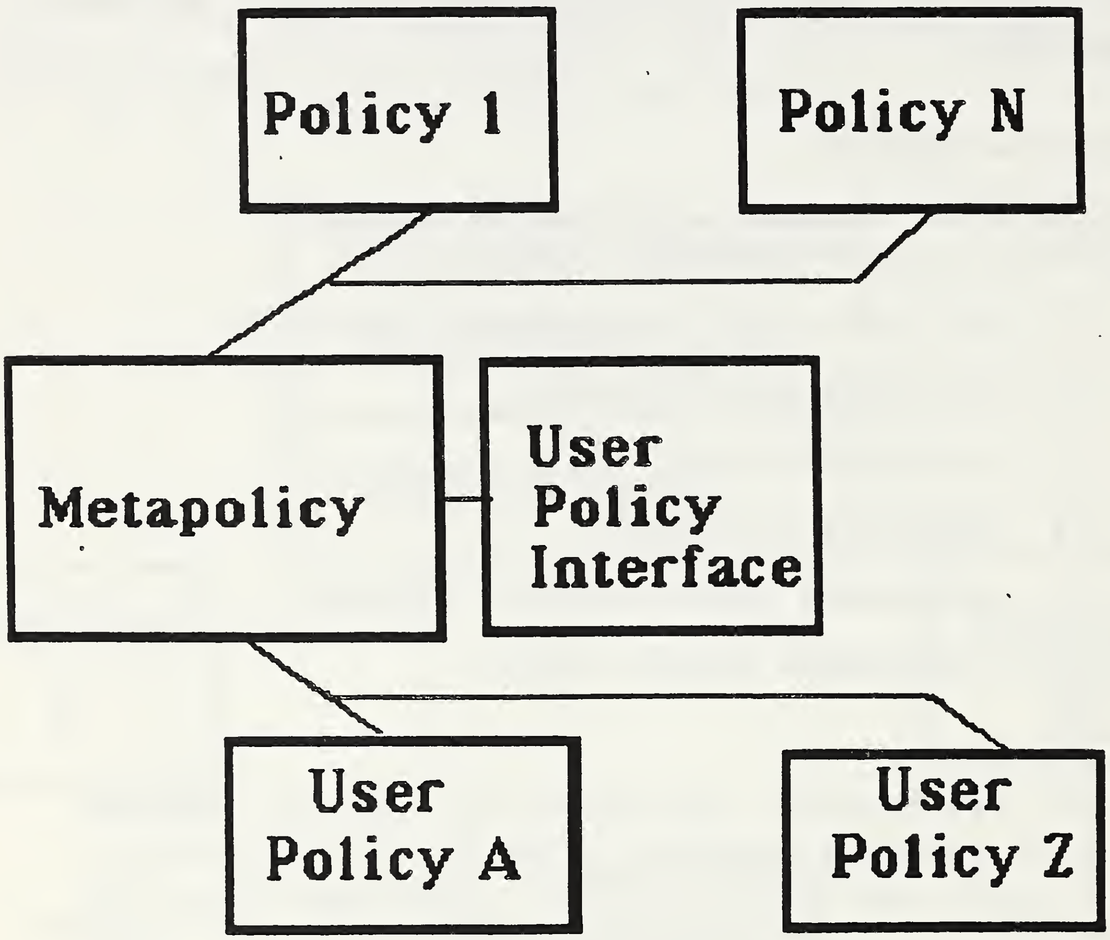
Several researchers, including Page, Heaney, Adkins, and Dolsen of Planning Research Corporation[2] and Abrams, LaPadula, Eggers and Olsen of MITRE[3], have been exploring Rule-Based access control policies. The Rule-Based concept permits security policies to be implemented as sets of rules, and modified as needed without modifying the architecture of the secure system. This promising approach

[2] Page, John, Jody Heaney, Marc Adkins, Gary Dolsen, "Evaluation of Security Model Rule Bases", Proceedings of the 12th National Computer Security Conference, Baltimore, Maryland, 1989.

[3] Abrams, Marshall, Leonard LaPadula, Kenneth Eggers, Ingrid Olson, "A Generalized Framework for Access Control: An Informal Description", Proceedings of the 13th National Computer Security Conference, Washington, D.C., October 1990.

has been formally modelled by Dr. La Padula[4]. The Multipolicy Machine could be built upon multiple sets of rule-based access control policies implemented in software or firmware. The major difference from the single-policy approach is that there are multiple sets of rule-based policies, and the data's security label(s) indicate which ones apply to it.

The major advantage of the rule-based approach is that separate sets of rules could be set aside for the users. Each set would be a separate policy which the user authorities could modify as desired isolated from the rest of the trusted system.

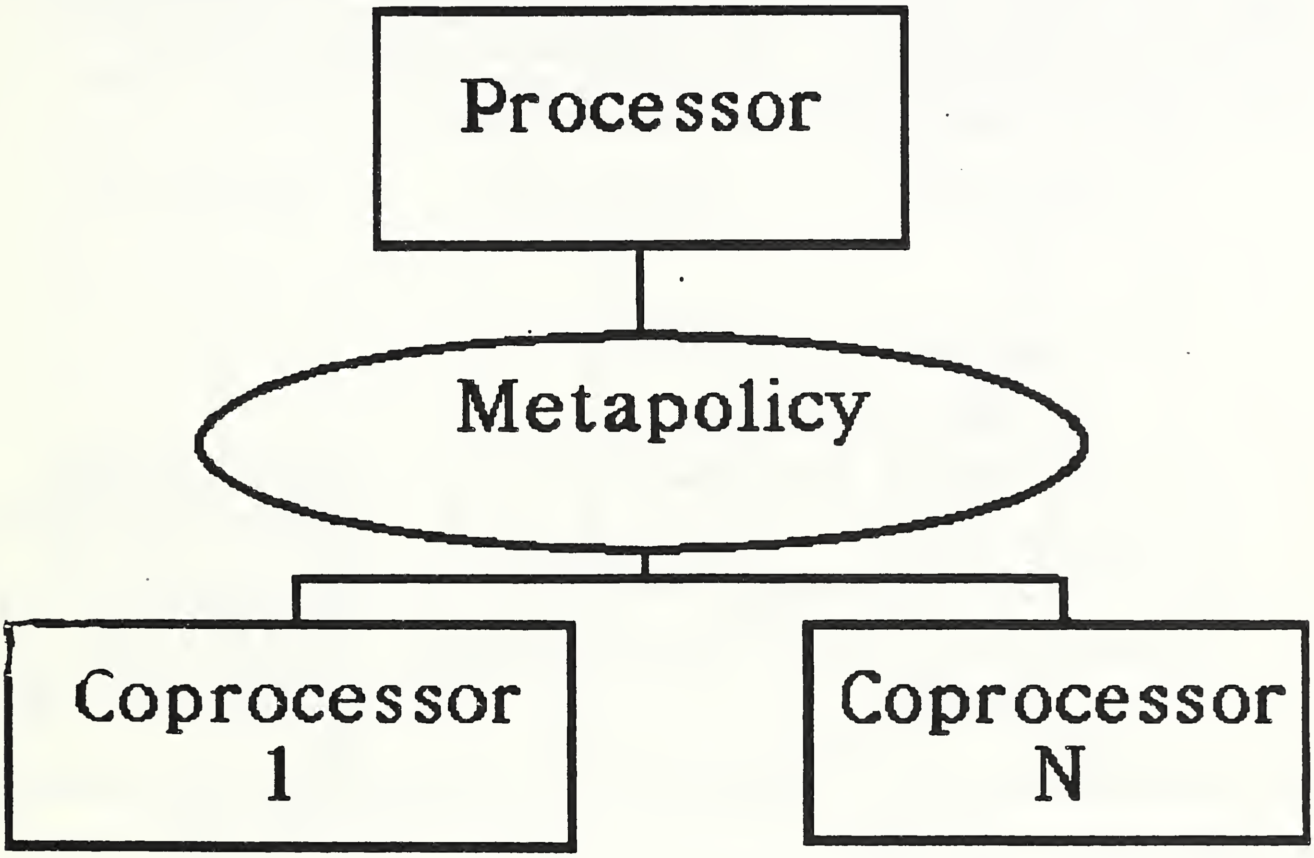


RULE-BASED

[4] La Padula, Leonard, "Formal Modeling in a Generalized Framework for Access Control ", <u>Proceedings of the Computer Security Foundations Workshop III</u> , Franconia N.H., June 1990.

Multiple Co-processors.

A second approach is to use multiple coprocessors, such as LOCK (Logical Coprocessing Kernel), to implement multiple policies. Although LOCK has an integral built-in security policy, its Sidearm can be modified for different policies. A multipolicy machine could, in theory, be constructed out of many single-policy processors operating in parallel, improving processing speed.

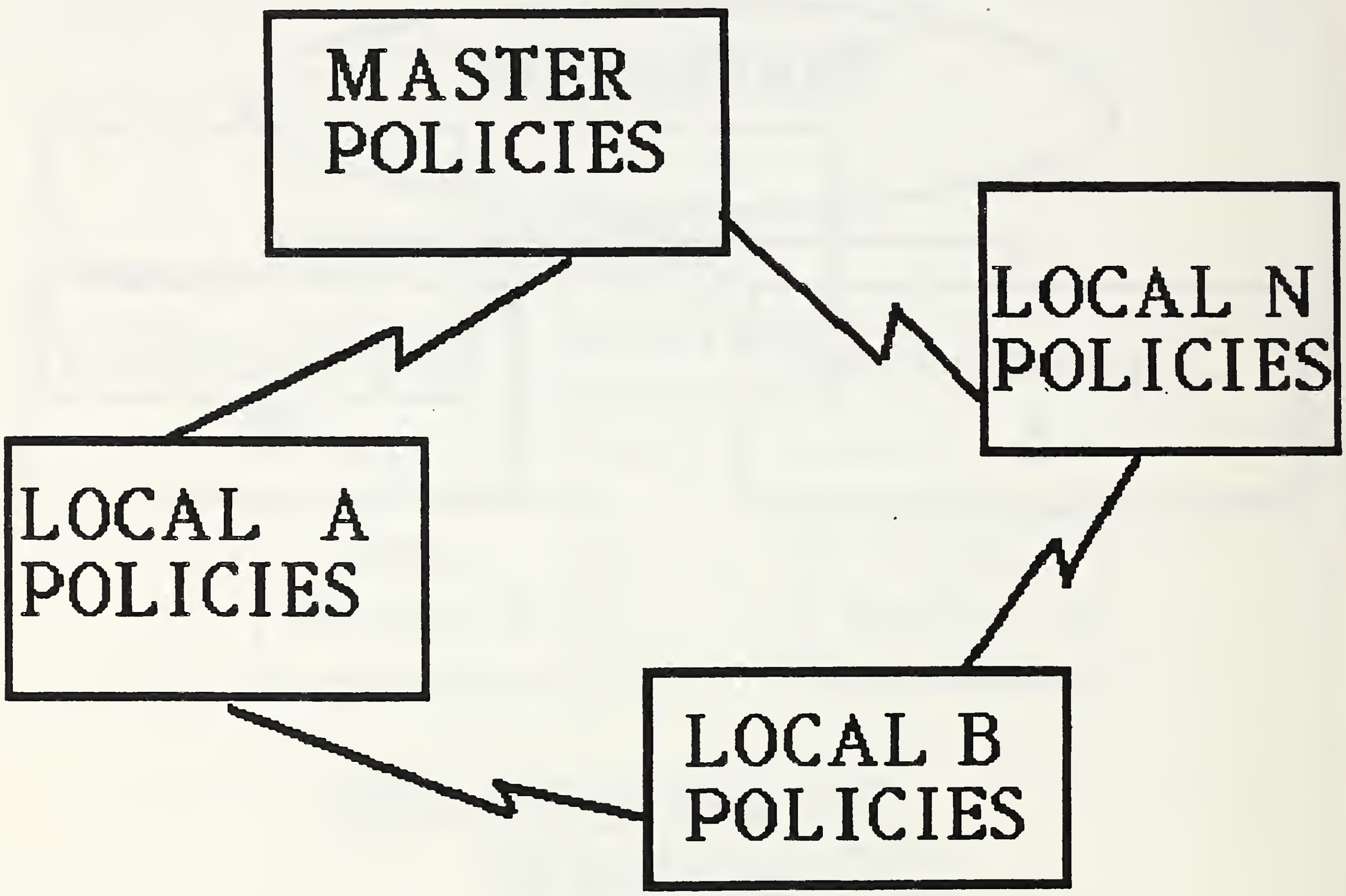


CO-PROCESSORS
(LOCK)

Distributed System.

A third approach is to use a distributed system where each machine implements a local security policy, and data whose sensitivity prevents it from being processed on one machine is forwarded to another. This approach could be used with current trusted equipment, although it wouldn't be very efficient.

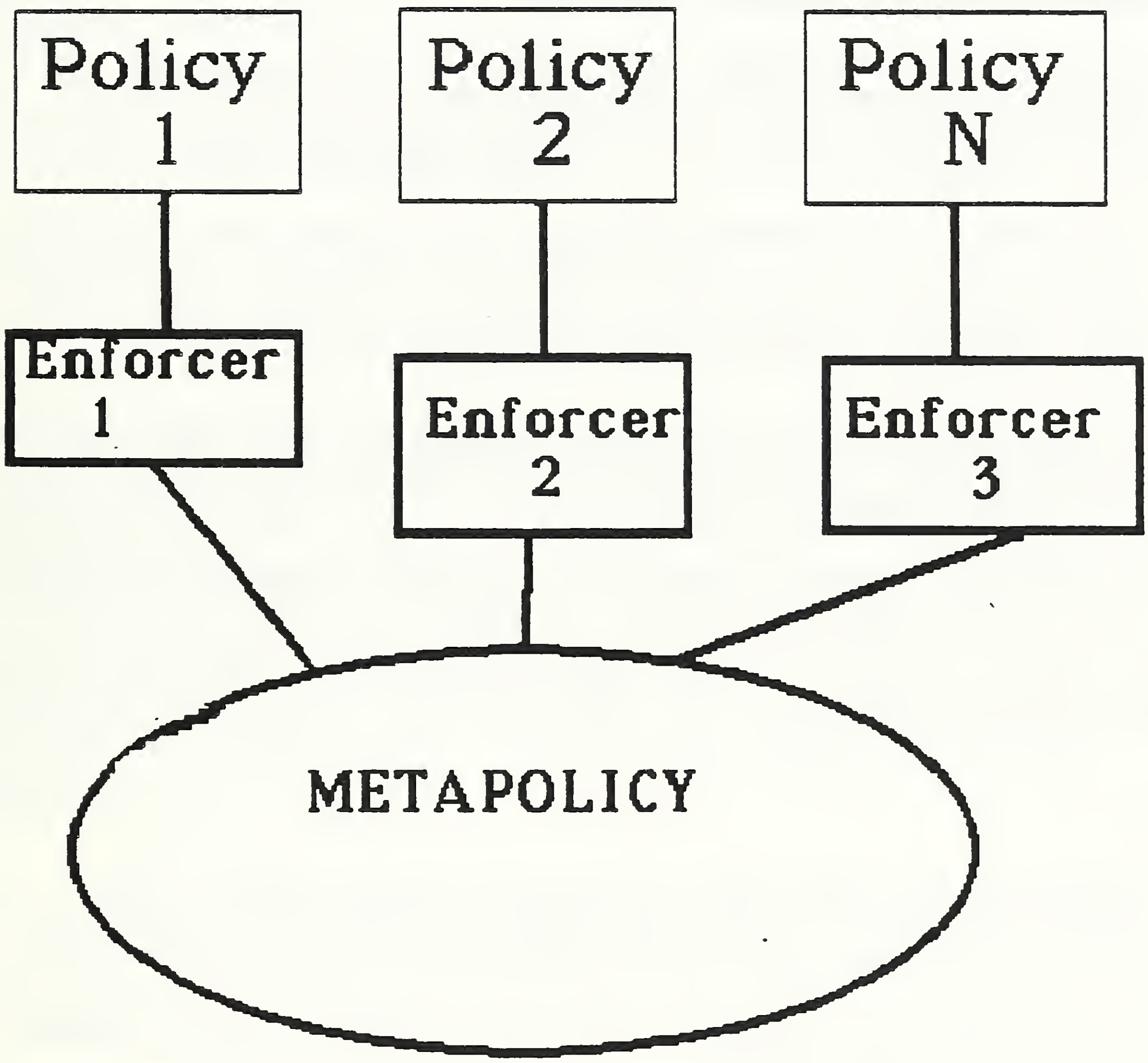
For efficiency, each local machine should implement all the local security policies, and data which doesn't come under the local policies would be forwarded to a remote node for policy enforcement. The distributed approach assures that local policies will be applied quickly, without losing the capability for enforcing rare policies.



Parallel Processors.

Very large scale integrated circuits (VLSI) make it possible to build trusted systems in hardware. Processors on a chip make it possible for each policy and its enforcer to operate in parallel with other policies and enforcers.

PARALLEL PROCESSORS



Hybrids.

Many combinations of the above techniques would be possible, as illustrated with the second distributed example. Other approaches not mentioned here are possible as well.

Metapolicies Revisited

A metapolicy is a set of rules about policies. It includes who can set policy, who can change policy, and what the procedures are for changing policies. It includes rules about developing, verifying, and protecting security policies. In the case of a multipolicy machine, a metapolicy includes rules for which policies have precedence over others and how to resolve policy contradictions that arise. We will focus on the metapolicies that are specific to multipolicy machines.

The basic metapolicy questions are:

1. What are the different ways that multiple policies may be permitted to interact? A hierarchical arrangement, a serial arrangement, parallel arrangements, overlays, and circular arrangements are some of the possibilities.

2. What are all the precedence possibilities? If policies are arranged hierarchically, should the enforcer start at the top or bottom of the policy pyramid? Should lower level policies 'inherit' higher level policies, as in object-oriented programming?

3. How can the precedence rules be encoded into the system so that some rules are encoded by the vendor and others by the site System Security Officer?

4. How can the metapolicies be certified? Should they be included in informal and formal models?

5. How should control be maintained after data is sent to a security policy?

ISSUES

There are several important questions to ask about the Multipolicy Machine. Here are some anticipated questions, and possible answers to the concerns expressed.

Q. Will the National Computer Security Center (NCSC) accept the multipolicy paradigm?

A. If the details are sufficiently worked out to prove that it is secure, the NCSC would welcome a more flexible new paradigm, especially if it does not invalidate the excellent work in security accomplished to date.

Q. Can the Multipolicy Machine be proven to be secure?

A. Yes, but more work is needed. The Electronic Systems Division of the U.S. Air Force plans to fund a feasibility study of the Multipolicy Machine via a Small Business Innovation Research (SBIR) Phase I grant to Data Security Inc. Starting in July 1991, we will explore these and other issues.

Q. Several national and international agencies (ECMA and ISO, for example) are working on sensitivity label standards to make information interchange easier between MLS systems. Can the Multipolicy Machine incorporate these evolving standards?

A. Yes. The Multipolicy Machine fits very nicely with the European standards.

Q. Can we design a Multipolicy Machine which is simple to manufacture, evaluate, and accredit? Can commercial off-the-shelf components be used?

A. I hope the answer to both questions is yes, but need more time to engineer the technology.

Q. How much more complicated will it be to evaluate multiple instead of single policy machines?

A. Although initially more difficult, it will eventually be easier to evaluate multiple policy machines than single policy machines because the policy will be separate from the mechanisms. Now, policy and mechanisms are integrated and must be evaluated together. When rule-based or other machines which separate policy from mechanism are accepted, it will be sufficient for the vendor to prove to the evaluators that their mechanisms implement any of a set of security policies. Proving that the particular policy of a particular installation is valid and supported by the mechanism is left to the certification and accreditation process.

Q. The US enforces export controls on state-of-the-art technology. Since the Multipolicy Machine will be valuable in multinational environments, should the machine be targeted at a level below B3 to avoid export controls? What are the implications?

A. The Multipolicy Machine will be most useful in networks, which require higher levels of either computer or physical security. I anticipate that the Multipolicy Machine will be first built in Europe where the need to cross security domain boundaries is well established and understood.

CONCLUSIONS

The multipolicy machine is a paradigm which could be successfully implemented in many ways. It will provide greater flexibility for users who need to add their own security policy specifics to the security policy of an existing system. It will make it easier to transfer data to systems in other security policy domains. It will let users model complex real world security policies more easily and permit contradictory policies to operate in parallel. Parallel processing may permit an improvement in trusted system performance, as well.

The multipolicy machine is now just a concept. Much more work needs to be done to make it a reality.

REFERENCES

Abrams, Marshall, Leonard LaPadula, Kenneth Eggers, Ingrid Olson, "A Generalized Framework for Access Control: An Informal Description", *Proceedings of the 13th National Computer Security Conference*, Washington, D.C., October 1990.

Biba, K.J., April 1977, *Integrity Considerations for Secure Computer Systems*, ESD-TR-76-372, MTR-3153, Rev. 1, Electronic Systems Division, Air Force Systems Command, United States Air Force, Hanscom Air Force Base, Bedford, Massachusetts.

Department of Defense Trusted Computer Systems Evaluation Criteria, December 1985, DOD 5200.28 STD.

European Computer Manufacturers Association, *Security in Open Systems, A Security Framework, ECMA TR/46*, July 1988.

Hosmer, Hilary H. "Integrating Security Policies", *Proceedings of the Third RADC Workshop of Multilevel Database Security*, Castile, NY, June 1990.

LaPadula, Leonard, "Formal Modeling in a Generalized Framework for Access Control", *Proceedings of the Computer Security Foundations Workshop III*, Franconia, N.H. June 1990.

Page, John, Jody Heaney, Marc Adkins, Gary Dolsen, "Evaluation of Security Model Rule Bases", *Proceedings of the 12th National Computer Security Conference,* Baltimore, Maryland, 1989.

"Modelling Security Policy and Labelling Unclassified but Sensitive Information - A Canadian Perspective" (Position Paper), D.S. Crawford (Canadian Department of National Defence)

Modelling Security Policy and Labelling Unclassified but Sensitive Information - A Canadian Perspective [1]

D.S. Crawford
Directorate of Security Operations
Department of National Defence
101 Colonel By Drive
Ottawa, Ontario
Canada K1A 0K2

1 Introduction

1.1 For eons, humanity has operated within a hierarchical policy framework. Succinct and broadly applicable policy statements are interpreted and elaborated until the bare bones are sufficiently fleshed out that an orderly and commonly understandable set of directions, procedures and guidelines exist and society as a whole can act upon the policy statement. Security policy adheres to this general model of behaviour. An added complication that has occurred in recent times is the necessity to develop detailed, unambiguous sets of rules such that the policy can be reflected in an automated fashion.

1.1.1 These models of policy must, in order to be effective, accurately reflect the existing policy. Modelling the well established and internationally recognised security policy surrounding classified information has become well known and an extensive body of literature has developed that addresses this. Labelling information is a component of such a model.

1.1.2 The development of a security policy to address unclassified but sensitive information is neither uniform nor well developed. This state of affairs is

---

[1] The statements expressed within this paper are the opinions of the author and are not to be construed as an official Government of Canada or Department of National Defence position.

due to the widely varying needs of widely disparate interest groups. The categorization, marking, protection required and personnel clearances required differ wildly from firm to firm and nation to nation, if in fact a formal policy exists at all. This contrasts to the extremely stable, well defined world of classified information with a very small, universally recognized set of levels of hierarchical sensitivities. Given the nature of the realm of unclassified but sensitive information, it may be assumed that modelling such a policy to conform with frameworks developed for the classified realm will be problematic, if even possible.

1.1.3 This paper discusses the policy of the Government of Canada (GOC) concerning unclassified but sensitive information and shows the inadequacies posed by an existing policy model, a monolithic confidentiality model, when attempting to model an actual policy that addresses both classified and unclassified but sensitive information.

2 Background

2.1 Relevant Canadian Legislation

2.1.1 Security policy is, in most part, a codification of the requirements imposed by existing statutes and laws. Two federal legislative Acts enacted in the 1980's brought about a significant change in the federal government responsibilities in addressing the individual's right to information.

2.1.2 The Privacy Act provided individuals with access to their personal information held by the federal government and protected individuals' privacy by limiting those who could access this information, thus returning some control to the individual over the collection and use of personal information by the federal government. In addition, a Privacy Commissioner, reporting directly to Parliament, was established with a mandate to audit compliance with the Privacy Act and to investigate individual complaints.

2.1.3 The Access to Information Act addressed the other aspect of rights to information, by providing individuals with the right of access to information not explicitly protected by the Privacy Act. An Information Commissioner, reporting directly to

Parliament, was established with a mandate to audit compliance with the Access to Information Act and to investigate individual complaints.

2.2 The Government Security Policy

2.2.1 The promulgation of the Government Security Policy (GSP) in 1986 introduced the concept of unclassified but sensitive information, identified as "designated information," as a stated Government of Canada policy [1]. This was a significant shift from the age old approach of classifying all sensitive information.

2.2.2 The new policy established a two step approach based on an injury test. Information, whose unauthorized disclosure or other compromise that could reasonably be expected to cause injury to the national interest, that was sensitive in the national interest, was classified. The levels of classification, Confidential, Secret or Top Secret, were based on the extent of damage. Information, whose unauthorized disclosure or other compromise that could be expected to cause injury to interests other than in the national interest, was identified as designated information. The levels of designation, as identified in the GSP, were "sensitive" and "particularly sensitive." Classified and designated information was to be identified as such with reference to specific provisions of the Access to Information Act and the Privacy Act in order to be exempt from disclosure under these acts. Information that was neither classified nor designated remained Unclassified.

2.2.3 Government institutions were required to mark all designated information with the term "Protected." In addition, an institution could, at its discretion, add the suffixes "A", "B", and "C" to indicated sensitive, particularly sensitive and extremely sensitive information. Therefore three types of designated information, Protected A, Protected B, and Protected C, were established to mark the various levels of designated information in a manner analogous to the marking of classified information. Government institution were required to provide adequate protection for designated information, which directly related to the sensitivity of the information. The physical protection required for Protected A, B and C roughly corresponded to the physical protection required for classified information at the Restricted, Confidential and Secret levels, respectively.

2.2.4 The addition of designated information caused additional changes in more than just document marking and storage. Personnel clearances were affected as the rationale for requiring a security clearance changed. The former practice of requiring a security clearance had to be limited to only those requiring access, on a regular basis, to classified information. There was no longer as many positions requiring clearances since there was no longer the vast numbers of employees with a "need to know" requirement for classified information. This was perceived as a cost saving measure, since it would reduce the number of security clearance investigations required to be conducted by security staffs.

2.2.5 A requirement existed, however, to establish a level of trust for employees who did not require access to classified information but had access to designated information and valuable assets. Personnel screening was established at two levels. The Basic Reliability Check was established for access to sensitive assets. The Enhanced Reliability Check was established as a requirement for employment for periods exceeding 6 months and was required for access to designated information.

3 Impact on Departmental Policy

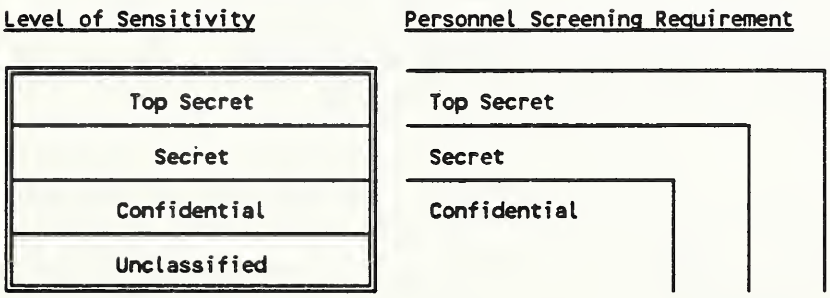
3.1 Policy Implementation Within Departments

3.1.1 The impact of the sweeping revisions to the identification of sensitive information varied among the federal departments. The Department of National Defence (DND), long used to the necessity of protecting information, easily adapted by establishing a 1:1 mapping from existing practices. The three levels of designated information, Protected A, Protected B and Protected C, could essentially be mapped to non-national interest information that had been previously classified Restricted, Confidential and Secret, respectively. Other departments implemented the policy in slightly different manner, such as the use of "Protected-Taxation" to correspond to "particularly sensitive".

3.1.2 Modelling the Government Security Policy

3.1.2.1 In order to conform to the GSP, automated systems would be required to model the policy. In the case of systems operating in a Dedicated or a System High Security Mode of Operation, the management of the additional types of sensitive information was addressed through manual means of labelling information. In the case of systems operating in a Multi-Level Security Mode of Operation, system labels would have to be developed to address the new types of sensitive information.

3.2 Prior to the adoption of the policy recognizing designated information, a model representing the policy had been constructed that supported various labelling schemes. Following the Bell and Lapadula model of confidentiality [2], a model could be depicted to portray the increasing level of sensitivity, as:



Classified / Unclassified Model

Labels could then be associated with each level indicated on this model. Since the model conformed to the policy concerning classified information and accurately reflected the increasing levels of sensitivity, the increasingly restrictive levels of physical protection and increasingly extensive personnel clearances, it was accepted as a means to implement the policy.

3.3 The policy concerning designated information, as interpreted within the Department of Defence, also may be modelled in a similar manner. Following the Bell and Lapadula model of confidentiality, a model could be depicted to portray the increasing level of sensitivity, as:

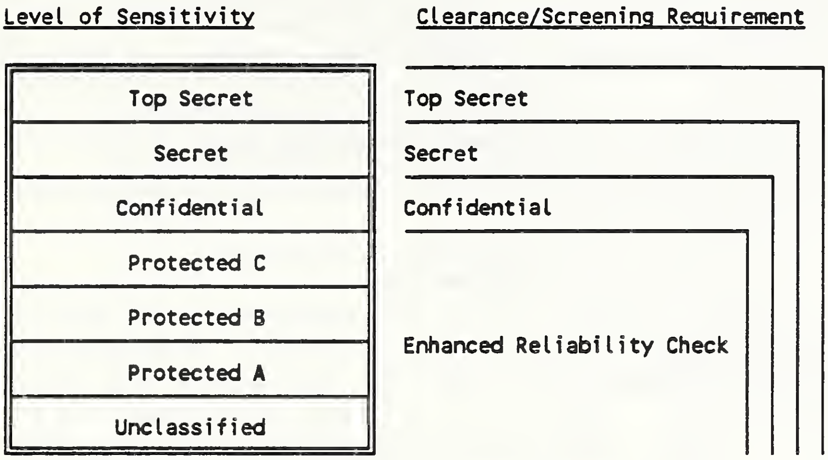
Level of Sensitivity	Personnel Screening Requirement
Protected C	Enhanced Reliability Check
Protected B	
Protected A	
Unclassified	Basic Reliability Check

Designated / Unclassified Model

This model conforms to the policy concerning designated information and accurately reflects the increasing levels of sensitivity, the increasingly restrictive levels of physical protection and increasingly extensive personnel screening.

3.4 Monolithic Policy Models and Existing Policy

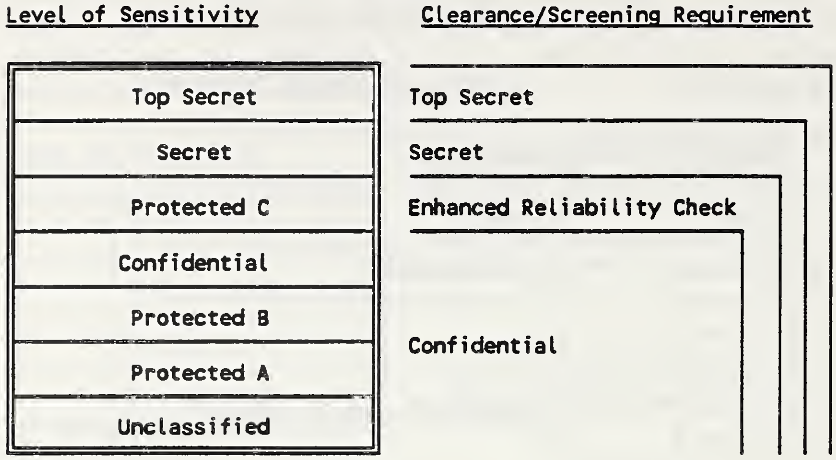
3.4.1 Current automated information systems capable of representing multiple levels of confidentiality sensitivity only support a monolithic model described in terms of ordered hierarchical levels and additional non-hierarchical categories. Following the Bell and Lapadula model of confidentiality, a model could be constructed to portray the policy required by the GSP, in increasing level of sensitivity, as:



Model 1: Classified and Designated Information

3.4.2 This model conforms to the policy concerning classified and designated information in that it depicts the increasing levels of sensitivity based on degree of damage of compromise. In addition, it accurately reflects the increasingly extensive personnel screening since a user who obtains a security clearance, such as Confidential, Secret or Top Secret, will have met the requirements of an Enhanced Reliability Check. It does, however, fail to accurately depict the physical protection required for Protected C information, since it implies that this information would be physically protected, at best, at a level commensurate with Confidential whereas the policy requires that this information be protected with the same physical protection as Secret. In an AIS based on the Bell and Lapadula model, an object containing Protected C information could be imported into a Confidential object. This is clearly a security breach, as such an object would be afforded a level of physical protection inappropriate for the sensitivity of the information. This model is therefore unacceptable.

3.4.3 A second model, to address the physical protection of Protected C, could be constructed as:

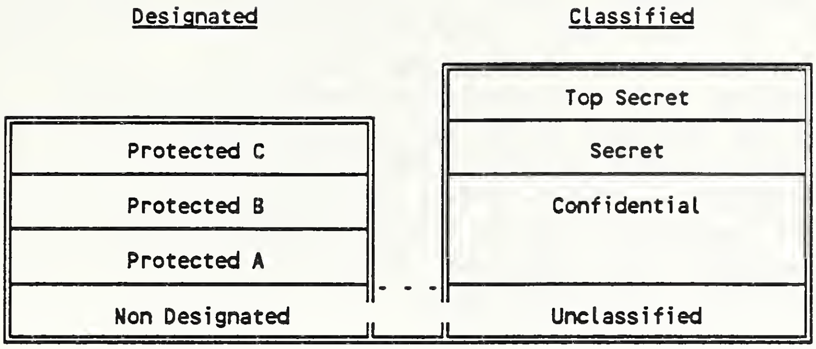


Model 2: Classified and Designated Information

3.4.4 This model conforms to the policy concerning classified and designated information in that it depicts the increasing levels of sensitivity based on degree of damage of compromise and that it accurately reflects the increasingly restrictive physical protection required. It does, however, fail to depict the personnel clearance and reliability check screening requirements. The ordering of levels in this model would mean that, in an AIS based on a Bell and Lapadula policy model, an individual with only an ERC may have access to Confidential information. This is clearly a security breach, as a security clearance is required for access to classified information. This model is also unacceptable.

3.5 The Disjoint Policy Model

3.5.1 Since neither model can adequately model the security policy, it can be concluded that a monolithic policy model is not appropriate for the existing policy in question. This suggests that a monolithic model, as supported by current labelling schemes, may not represent the general case. An alternative approach would be to represent the policy model as a series of hierarchical confidentiality "stacks", which I shall refer to as a disjoint policy model. This model would depict the GOC security policy by addressing classified and designated information as separate, or disjoint, submodels within the confidentiality model.



Disjoint Policy (Confidentiality) Model

3.5.2 Since the purpose of this model was to address weaknesses identified in the previous models, it also must be examined to determine if this model adequately addresses the existing policy. Individuals without appropriate clearances will be denied access to sensitive information by this model. Access to classified information would be restricted to individuals holding appropriate clearances. Access to designated information is now distinct from access to classified information and the only linkage is the indirect linkage that a user holding a security clearance implicitly holds an ERC. In terms of physical protection, this model no longer links increasing levels of protection for designated information with the levels of protection for classified information. By removing the linkage, the model will support protection requirements for designated and classified that cannot be rank ordered.

3.5.3 In terms of labelling, this model would require that an object refer to label components addressing classification and designation. The problem inherent in Model 1, the importation of less sensitive information, would be avoided since an object labelled with a classified sensitivity level would be required to include a designated sensitivity level in order to avoid non-comparable labels. One could draw a parallel to the current use of levels and categories. In this context, an object could have <u>n</u> categories, where each category was assigned a sensitivity level. The non-comparability of categories would serve to maintain the distinction between the various types of sensitive information and each category could be used to represent a different and non-comparable security policy, such as one policy component of confidentiality, integrity or availability.

3.5.4 This model maps well to the existing document based world. Within DND, documents shall have paragraph and page level sensitivity markings [3]. Paragraphs containing both classified and designated information are to be marked with both markings, such as "(PC-S)" for a paragraph containing Protected C and Secret information. This model would support a comparable type of marking since both classification and designation information could be carried simultaneously within the same objects.

4 Conclusions

4.1 The history of marking and otherwise labelling information has, until very recent times, focused exclusively upon the realm of classified information. Existing products and protocols have been developed to support a monolithic model of confidentiality labelling due to market demands. Recent developments would seem to indicate that this monolithic model may not be adequate to represent all possible security policies.

4.2 The specific case of mapping the existing Government of Canada security policy to a label based confidentiality model provides an illustrative example of an existing security policy that cannot be modelled as a monolithic model. The existence of such real world policies poses a challenging problem to systems designers and implementers in specifying and developing products and protocols which are sufficiently general to be able to handle policy models that do not conform to a monolithic model.

References

1. Treasury Board of Canada, Security Policy and Standards, November 1990.

2. Bell, D.E., and LaPadula, L.J., "Secure Computer System: Unified Exposition and Multics Interpretation", MTR-2997, The Mitre Corporation, March 1976.

3. Department of National Defence, A-SJ-100-001/AS-000 - Security Orders for the Department of National Defence and the Canadian Forces, May 1989.

"The Need for Release Markings in the GOSIP Standard Security Label" (Position Paper), Tom Bartee (IC Staff)

POSITION PAPER ON THE NEED FOR RELEASE MARKINGS IN THE GOSIP STANDARD SECURITY LABEL

This is a position paper concerning the use of inverted bit-map release markings as a mechanism for labeling classified data in the Standard Security Label for the Government Open Systems Interconnection Profile. The position taken is that because of the widespread usage of release attributes in Government systems inclusion of this labeling technique would be desirable.

Examples of release attributes include country and NATO release markings, markings for release to selected contractors (corporations) in certain programs, releases to LEAs and DEA in DOD and Intelligence counter-narcotics programs, etc.

When two bit-map markings for (normal) restrictive attributes are combined, the two bit-maps are ORed bit-by-bit as follows.

```
0110 + 1010 --> 1110
||||   ||||     ||||
ABCD   ABCD     ABCD
```

this gives a lattice least-upper-bound. For the above the leftmost label shows B and C attributes and the rightmost A and C attributes so the resulting label should indicate the combined attributes A and B and C.

When ORing is tried for release attribute markings it does not give the desired result.

```
0110   1010 --> 1110
||||
ABCD   ABCD     ABCD
```

The above indicates that a label indicating a release to B and C when combined with a label indicating a release to A and C provides for release to A and B and C while, in fact, the release should be to C only.

If inverted bits are used where a 0 indicates a release and a 1 the absence of a release, the result is

```
1001   0101 --> 1101
||||
ABCD   ABCD     ABCD
```

The leftmost label is for release to B and C and the middle label indicates a release to A and C, the result is that the object is releasable only to C which is what is desired.

The inverted bit-map markings can also be used in implementing Mandatory Access Control. The user is given a label with 0s in the positions where the release attribute markings indicating his affiliations occur (if the user is British a 0 is in the British position, if employed by Boeing a 0 is in the Boeing position, etc.) and 1s are placed in the other positions. When the label associated with a user is ORed with a label on a data item, the presence of a 0 in the result indicates the data has been released to the user.

The inverted bit-map technique has been used in several operational systems and is included in the DCI Extended Security Option for the IP header. It is also used in the CMW program. Its virtue is its simple operation and conceptual neatness. While labels can be used with non-inverted release markings, programs must "know" which bits are the release bits and process them differently.

The inclusion of an inverted bit map marking scheme for release attributes as one of the Security Tag Types in the standard would be useful to a large body of Government (and Commercial) users.

"The Amdahl Approach to Security Labels" (Position Paper),
Jon Graff, Ph.D.

The Amdahl Approach to Security Labels

Jon Graff, Ph.D.

I. Security Policies

Security Policies form the foundation for the architecture and design of a Trusted Computer Base (TCB) or a Trusted Computer system or network. The policy defines the philosophy and methods for obtaining and assuring security of the information and processes within the system.

The security policies set forth in the DoD Trusted Computer System Evaluation Criteria (Orange Book) and the DoD Trusted Network Interpretation (Red Book) are based on the trusted "reference monitor" concept. The reference monitor's function is to ensure that access is only permitted when the subject's and object's label meet the requirements set forth in the security policy. The concept calls for the trusted reference monitor to examine "labels" to determine if a "subject" (an active agent, such as a calling program or a human) has permission to access an "object" (passive resource such as a piece of data). The subject's label indicates the characteristics that an object must have in order for a subject to be permitted to access the object. The object's label identifies what characteristics the subject must have in order to be permitted to access the object.

A. The Bell and LaPadula Family of Security Policies

The Bell and LaPadula family of security policies (BLFSP) are based on a reference monitor that requires sensitivity-levels as a mechanism for policy inforcement. The model is based on the environment in which multiple subjects may have access to multiple objects. The reference monitor adjudicates the access control between subjects and objects by comparing their "sensitivity labels" according to the Mandatory Access Control (MAC) policy. The reference monitor permits a subject to access an object only if the subject's and object's sensitivity labels fulfill the requirements of the security policy.

The important point of this discussion is that sensitivity labeling is a required part of maintaining the BLFSP.

B. The Amdahl 5995A Trusted Multiple Domain Feature (TMDF) Security Policy

In contrast to the more familiar BLFSP, the Amdahl 5995A Trusted Multiple Domain Feature (TMDF) Security Policy is "Isolation" which is enforced by the mechanism of "Separation." A scholarly description of the isolation security philosophy using separation can be found in a paper by Rushby (J.M. Rushby, "Proof of Separability: A Verification Technique for a Class of Security Kernels," Computing Laboratory, University of Newcastle upon Tyne, May 5, 1981). The Rushby Isolation policy requires that each subject is segregated with its objects from any other subject and that subject's objects.

In the Amdahl TMDF, the isolation security policy is manifested in the fundamental architecture of the machine. Simply stated, the TMDF permits a single computer to be split into up to seven separate and distinct operating environments, called "Domains", each containing a separate, distinct and totally independent operating system. The operating systems within the Domains are referred to as System Control Programs (SCPs). The Domains co-exist on the computer under the supervision of the TMDF. The TMDF enforces the separation of each of the Domains by giving each Domain a unique time slice of the CPU as well as assigning each Domain its own set of resources such as storage, channels and Input/Output Configuration Data Sets (IOCDSs). During its time slice, the Domain and its SCP have exclusive use of the computer facilities and the Domain's resources (CPU, storage, channels and IOCDSs). Additionally, once the TMDF assigns a resource to a Domain, that Domain maintains sole and exclusive possession and access to that resource until the TMDF oversees that resource's release.

The SCP believes it has sole possession of the entire computer. When the Domain's time slice expires, the TMDF puts the SCP and its Domain into a state of "suspended animation". At the beginning of a time slice, the TMDF reactivates the Domain and the SCP into the exact same active state the Domain and the SCP were immediately prior to being placed into suspended animation.

In summary, the TMDF security policy is Isolation. Therefore, it is the TMDF's responsibility to ensure that each Domain, and therefore its respective SCP, is kept totally separate and without knowledge or access to any other Domain's resources.

C. Comparison of the BLFSP and the Rushby Policy

The Rushby policy of Isolation as implemented in the TMDF security model does not have the same requirements as the BLFSP. Both obtain Mandatory Access Control (MAC) but through different mechanisms. The TMDF ensures MAC by total separation, i.e., the TMDF's MAC is Separation. In contrast, BLFSP's MAC requires the adjudication of the sensitivity labels of the subjects and the objects.

Table I shows the two types of Security Labels. The BLFSP requires Sensitivity labels, whereas the Isolation policy requires "Separation" labels. Important points to note:

- o Sensitivity labels are NOT required for the TMDF model because the TMDF model is based on Separation.

- o The individual SCPs, within the TMDF, define their individual security policies. An SCP may base its security policy on one of the policies in the BLFSP. Therefore the individual SCPs may require sensitivity labeling. However, it is very important to note that the operations within the SCP are out of the purview and responsibility of the TMDF.

II. The Labeling Issue

A. Traditional "Sensitivity labels" supporting the reference monitor model

The BLFSP require sensitivity labeling. Sensitivity labeling has two aspects, a hierarchical part and, if required, a subservient, non-hierarchical part. The hierarchical part of the label refers to the classification level or "security sensitivity", e.g. Top Secret, Secret, and Confidential. The hierarchical classification levels define the security risk of the unauthorized release of the information. Within each classification level there may exist "compartments" which define areas of "the need to know" or access requirements. These compartments are "non-hierarchical" because they require the same clearance for access, however they each have a different "need-to-know" requirement.

In the BLFSP, each subject is assigned permission to access information or perform tasks based on the subject's security risk (classification level) and "need to know" (compartment). The same labeling is applied to objects. These sensitivity labels must be protected from unauthorized changes and therefore strict requirements are made on how the sensitivity labels are generated, used, monitored and protected. A Mandatory Access Control policy mandates the labels assigned in an automatic, prescribed manner.

B. The TMDF "labeling" solution

The TMDF does not have or need the traditional "sensitivity labels" to ensure Mandatory Access Control. TMDF ensures Mandatory Access Control by enforcing the strict separation of the Domains. TMDF separation begins at the time of Domain activation. At that time, the System Security Administrator assigns specific resources that the Domain may use. When the Domain receives a resource, the TMDF assigns the Domain's identity to that resource. The Domain's identity stays affixed to that resource until the Domain operator relinquishes the resource.

The Domain identifier which identifies which resources are assigned to which Domain is equivalent to Rushby's "colour." In Rushby's discussion each Domain has a different "colour" which is used to assist in separation. Thus the "colours" or TMDF Domain identifiers may be thought of as "Separation" labels. The TMDF separation policy permits resources to be available to more than one Domain, however only one Domain may possess a resource at a time. If a second Domain requests an already activated resource, the request is denied. The requesting Domain knows only that the resource is not available, not the cause of the non-availibility.

It must be emphasized that the TMDF does not need or require sensitivity labels to enforce the Mandatory Access Control through the security policy of Separation. In the TMDF, MAC is maintained with separation labels. The separation labels permit the TMDF to ensure that the Domains are totally separate and independent. The operation of the individual SCPs within the Domains are of no concern of the TMDF. Each SCP will have its own security policy and these SCP security policies (e.g., MAC policies) may require the traditional sensitivity labels.

Table I: Types of Security Labels		
Major Class of Labels	Sub-Labels	Function
Sensitivity		Used by the BLFSP Reference Monitor to determine if a subject should have access to an object.
	hierarchical	Indicate "classification level", e.g. Top Secret, Secret, or Confidential. These labels correspond to the security risk of having the information compromised.
	non-hierarchical	Indicate "compartments". Compartments are subgroups of a classification level (e.g. artillery, armor, infantry or Army, Navy and Air Force). These labels do NOT exist independently of the classification level.
Separation		Used by the TMDF reference monitor to determine if a Domain has possession of a resource.

Attendees List - NIST Invitational Workshop

Attendees List

Ken Alonge
Contel Federal Systems

Sun-Shin An
University of Korea

Thomas Bartee
Intelligence Community Staff

Dr. Dennis Branstad
NIST

C. Douglas Brown
Sandia National Laboratories

Chris Chiang
Hewlet Packard

Dave Claus
Department of Defense

David S. Crawford
Canadian National Defense Headquarters

Dr. Jonathan Fellows
Grumman Data Systems

Brad Gault
Allied Signal Corporation

Virgil Gibson
Grumman Data Systems

Paul Hammersley
Grumman Data Systems

Donald Heckman
Department of Defense

Hilary Hosmer
Data Security Inc.

Russell Housley
Xerox Special Information Systems

Richard Hovey
Digital Equipment Corporation

Wayne Jansen
NIST

Dr. Stuart Katzke
NIST

Larry Keys
NIST

Leroy Lacey
Informix Software Corp.

Larry Lunsford
Contel Federal Systems

Marc Mandel
Grumman Data Systems Division

Cathy McCollum
Unisys

Sammy Migues
Xerox

Mohammad Mirhakkak
The MITRE Coporation

Tassos Nakasis
NIST

Noel Nazario
NIST

Richard Parker
The MITRE Coporation

George Rogers
Intelligence Community Staff

Kristina Rogers
The MITRE Coporation

Robert Rosenthal
NIST

Ronald L. Sharp
AT&T Bell Laboratories

Arthur Sigues
NASA Headquarters

Maurice Smith
Allied Signal Aerospace

Larry Sudduth
National Capitol Systems, Inc.

Robert A. Tannert
Department of Energy Hdqtrs.

N. Vasudevan
IBM

Dale Walters
NIST

Dan Wilcox
National Security Agency

Roberto Zamparo
Swedish Telecom

NIST-114A (REV. 3-89)	U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	1. PUBLICATION OR REPORT NUMBER NISTIR 4614
	BIBLIOGRAPHIC DATA SHEET	2. PERFORMING ORGANIZATION REPORT NUMBER
		3. PUBLICATION DATE JUNE 1991

4. TITLE AND SUBTITLE

Standard Security Label for GOSIP
An Invitational Workshop

5. AUTHOR(S)

Noel A. Nazario

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

National Institute of Standards and Technology
Computer Systems Laboratory
Building 225/Room A216
Gaithersburg, MD 20899

10. SUPPLEMENTARY NOTES

☐ DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

On April 9 and 10, 1991 the Protocol Security Group at NIST held its Second Workshop on Security Labels. Forty representatives from the U.S. Government, Industry, and the Canadian Government gathered for two days to discuss a NIST proposed Standards Security Label for the U.S. Government Open Systems Interconnection Profile (GOSIP). Issues on security policy and security object registration were also discussed in reference to the proposed label. The information shared during the two days of discussion and the recommendations of the group are documented in these proceedings.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Computer Security Objects Register; Government Open Systems Interconnection Profile (GOSIP); Open Systems Interconnection; security labels

13. AVAILABILITY

- [X] UNLIMITED
- [ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
- [ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
- [X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES

132

15. PRICE

A07

ELECTRONIC FORM