Foreword

This document entitled *Threat and Risk Assessment Working Guide* provides guidance to an individual (or a departmental team) carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system. This document will help determine which critical assets are most at risk within that system, and leads to recommendations for safeguards that will reduce any risks to acceptable levels.

By following the guidance given therein, a TRA can be carried out such that it results in a concise report that:

- defines the IT system under assessment;
- states the aim of the assessment, along with the desired security level to be attained;
- identifies potentially vulnerable parts of the system;
- states the potential impacts of successful threat events on: the IT system; the business functions that the IT system supports; and the applications used to carry out the business functions, in terms of confidentiality, integrity and availability; and
- provides recommendations that would lower the risks to acceptable levels.

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
DSO	Departmental Security Officer
GSP	Government of Canada Security Policy
IT	information technology
RCMP	Royal Canadian Mounted Police
SEIT	Security Evaluation and Inspection Team
SoS	Statement of Sensitivity
TRA	threat-and-risk assessment

1.0 INTRODUCTION

1.1 Background

The Government of Canada Security Policy (GSP) requires federal departments and agencies to manage security risks—that is, the adverse effects that could result if security vulnerabilities were exploited—by first confirming the appropriateness of existing minimum security standards, and then supplementing those standards where necessary (while eliminating unnecessary expenditures and administrative barriers).

Risk management involves planning, followed by organizing, directing and controlling resources in order to ensure that risk remains within acceptable bounds. However, because it is prohibitively expensive—and probably impossible—to safeguard information and assets against all threats, modern security practice is based on assessing threats and vulnerabilities with regard to the degree of risk each presents, and then selecting appropriate, cost-effective safeguards.

Risk management is also a collaborative process, whereby representatives of affected groups have the opportunity to develop a shared understanding of security requirements and options. Such increased awareness also strengthens security, and makes it more compatible with user needs.

Managing risks requires defining:

- what is at risk
- the magnitude of each risk
- causal factors
- what to do about each risk.

Options for managing risk include:

- transfer
- avoidance
- acceptance
- risk reduction.

Note: *Risk reduction* can be achieved through the implementation of a managed system architecture that includes the following components:

- operational
- procedural
- physical
- personnel
- technical security.

Risk management for information technology (IT) systems presents some particular difficulties arising from the rapid evolution of technology. Failure to consider such factors in a timely fashion

could lead to ineffective (and/or unnecessarily costly) security measures. Therefore, risk management must be an integral part of a system's overall lifecycle.

The first step in the risk management process is the completion of a threat-and-risk assessment (TRA). (The GSP requires each government institution to conduct TRAs covering all of its classified and designated information and assets.) It is the task of the TRA analyst to determine the appropriate level of protection required for each type of asset, and to then present the findings to the Project Authority in a Risk Assessment Report.

1.2 Purpose

This document provides guidance to an individual (or a departmental team) carrying out a TRA for an existing or proposed IT system. It helps determine which critical assets are most at risk within that system, and leads to recommendations for safeguards that will reduce any risks to acceptable levels.

Since a Project Authority might initiate a TRA with little warning due to a situation causing major system security problems, one of the reasons for these guidelines is to help point the way in such a crisis. (The Project Authority should assign a manager who will be responsible for the project, and should provide the support that the TRA analyst/team will need to do the assessment.)

1.3 Scope

By following the guidance given herein, a TRA can be carried out such that it results in a concise report that:

- defines the IT system under assessment;
- states the aim of the assessment, along with the desired security level to be attained;
- identifies potentially vulnerable parts of the system;
- states the potential impacts of successful threat events on: the IT system; the business functions that the IT system supports; and the applications used to carry out the business functions, in terms of confidentiality, integrity and availability; and
- provides recommendations that would lower the risks to acceptable levels.

This document concentrates on the planning and the threat-and-risk assessment portions of Figure 1, below.

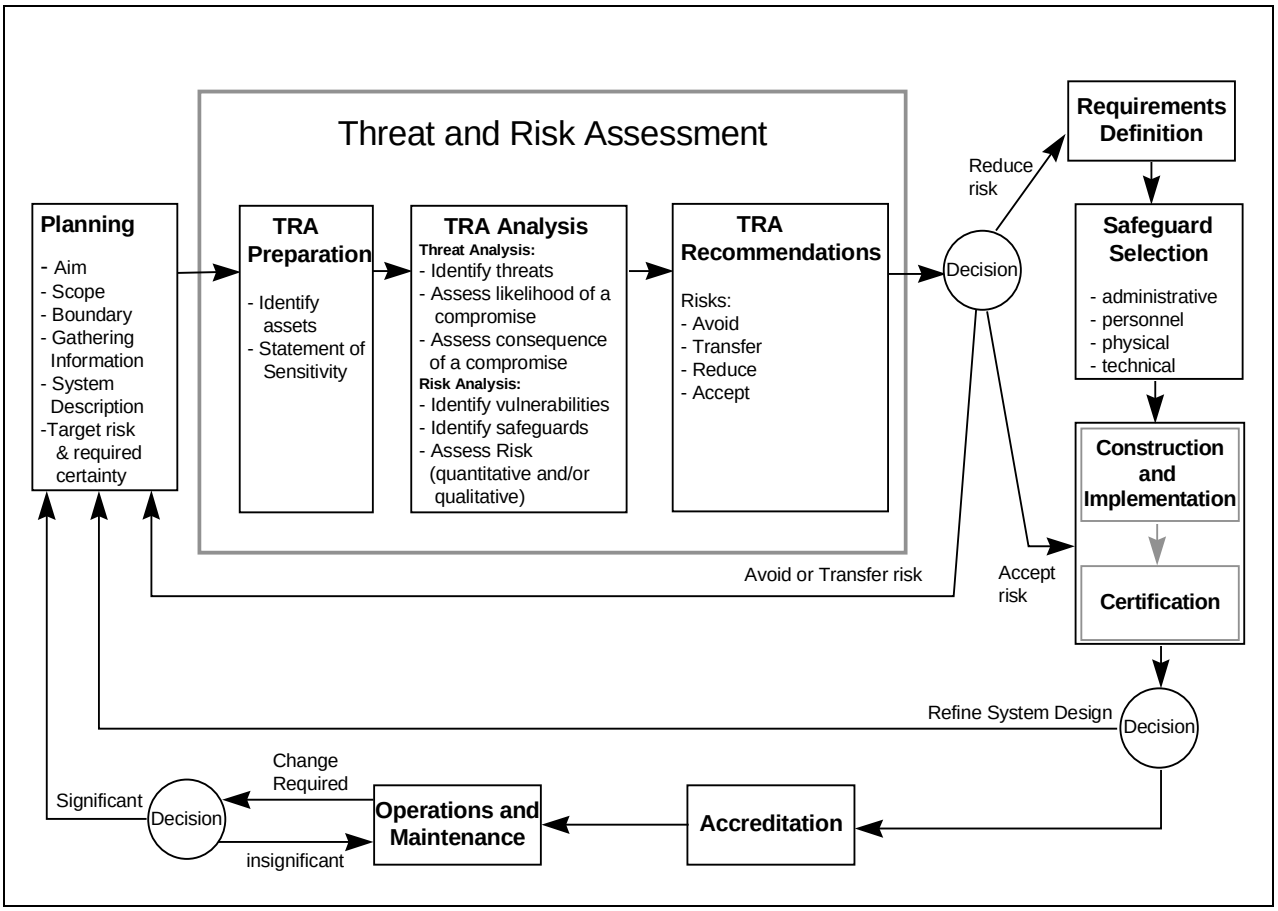

Figure 1 – Risk Management Model

The steps of the TRA process can be organized into nine major tasks, each associated with a document produced during the completion of that task. The major tasks comprise Section 2.0 of this guide. (These tasks and their associated documents are listed in Table 1, below.)

Each major task helps assess the value of the IT system in terms of both cost, and how critical it is to its supported business function(s). The form of each document depends upon the individual situation, but most documents provide input for one or more tasks that follow.

Note: It is always a mistake to continue beyond a task without completing the necessary documentation, and usually leads to a flawed TRA. Therefore, each step of the process requires constant attention to detail and completeness.

Table I – Tasks in the Threat-and-Risk Assessment process

TASK	Document Produced
TASK 1 Prepare and Plan	Work Plan, System Description, and Preliminary Statement of Sensitivity
TASK 2 Collect Data for Analysis	Initial Security Review
TASK 3 Analyze Policy and Standards Compliance	List of Non-Compliant Areas
Note: If an in-depth analysis is not required, the analysis may skip directly to Task 8.	
TASK 4 Perform an Asset Sensitivity Analysis	Statement of Sensitivity Report
TASK 5 Perform a Threat Analysis	Threat Analysis Report
TASK 6 Perform a Vulnerability Analysis	Vulnerability Analysis Report
TASK 7 Perform a Risk Analysis	Risk Analysis Report
TASK 8 Assess System Risks for Acceptability	Preliminary Risk Assessment Report
TASK 9 Deliver the Final Risk Assessment Report	Final Risk Assessment Report

This guide includes twelve annexes that contain supporting material useful in working through or understanding various steps of the TRA process:

- ANNEX A – Rating Tables
- ANNEX B – A Sample Description of a Typical IT System
- ANNEX C – Sample Questionnaire
- ANNEX D – Contents of a Statement of Sensitivity
- ANNEX E – The Level-of-Granularity Numbering Scheme
- ANNEX F – Sample List of IT System Assets
- ANNEX G – Sample List of Threat Agents
- ANNEX H – Sample List of Threat Events
- ANNEX I – Sample List of Vulnerabilities
- ANNEX J – Threats to Assets through Vulnerability Interrelationships
- ANNEX K – Glossary
- ANNEX L – Glossary Sources.

The rating tables provided in the annexes are to help users determine which areas should be considered critical.

Note: If at some point after the rating tables have been used the users should decide that security professionals are needed to perform a more detailed analysis, much of the work will already be done, and the security professionals can focus on the areas already identified as critical.

This guide is generic in its approach to the TRA process. If a "directed TRA" is called for in order to focus on a single or limited problem (for example, fraud, theft of PCs, or preventing the recurrence of an information leak), all of the material contained within this guide might not be required. However, the TRA elements would be essentially the same, and the steps that relate specifically to the issue of concern should be carried out.

2.0 STEPS IN THE THREAT-AND-RISK ASSESSMENT PROCESSS

This part of the guide contains nine subsections; each explains a major step of the TRA process in detail.

TASK 1 – PREPARE AND PLAN

(Documents produced: Preliminary Statement of Sensitivity, System Description, and Work Plan)

1.1 Understand the overall process.

The TRA process is normally initiated because of an identified need. (For example, a concern might have been raised because a recent threat event affected the IT system and/or the business process that is supported by that IT system.) In any event, the responsible manager (or another delegated person) issues an order for a TRA to be carried out on part or all of a specific IT system.

The most important aspect of a TRA is knowing exactly what it is that needs to be protected, and why. Inherent in this is the question of what constitutes the required level of security.

Normally, the responsible manager specifies:

- which IT system is to be assessed (that is, the boundary of the assessment);
- why the assessment needs to be done;
- the urgency or priority of the work; and
- the level of security required to accommodate the maximum acceptable amount of residual risk (for example, the maximum amount of time that a system may be down due to a particular threat event).

Annex J provides examples of the vulnerability interrelationships that can exist among threat agents, threat events and assets, along with possible consequences and some suggested safeguards.

1.2 Determine the scope of the threat-and-risk assessment.

1.2.1 Determine the level of analysis required, and how much detail should be in the final report.

The final report will need to be tailored to its audience. For example, the report might be a high-level analysis requiring decisions regarding further action to be made by appropriate authorities (senior management, etc.); or, it might be a detailed analysis completed for the level of management primarily responsible for the IT system.

Note 1: In instances where a detailed analysis is **not** required, the TRA assessment process can eliminate Steps 4 to 7, and proceed directly from Task 3 to Task 8.

Note 2: Sometimes there is a need to perform a "directed TRA" that focuses on a single or limited problem (for example, fraud, theft of PCs, or preventing the recurrence of a

specific information leak). These guidelines are **not** intended for such analyses. Engaging a security specialist for advice usually leads to better results when a directed TRA is called for.

1.2.2 Identify the required resources (time, funding, personnel, etc.).

1.2.2 Collect security policies and standards.

Collect: high-level policies and standards; local policies and standards; and business practices and procedures, from the Departmental Security Officer's (DSO's) support staff.

Polices and standards are the means of: enforcing a mode of behavior; enforcing a mode of operation; or measuring compliance to a specific security standard. They include the rules, directives and practices that govern how assets (including sensitive information) are managed and protected within an organization and its IT systems.

Note: This information can affect the focus of the analysis, especially if the analysis is being carried out on a very complex system.

1.2.3 Review the collected documents.

While reviewing the collected documents, identify and record any limitations that might affect the scope of the TRA, along with any assumptions that have to be made because of those limitations.

Some limitations that could restrict the scope of a TRA include: departmental security policies and standards; available resources; costs; and time limits. Such limitations could greatly affect the focus and the results of the analysis (especially of a very complex system), and might cause confusion for the recipients of the final report if they are not properly identified.

1.2.5 Revise the scope as required.

1.3 Identify the boundaries of the analysis.

Identify the physical and logical boundaries of the analysis by clearly outlining, at a high level, what the analysis should include.

- The physical system boundary should include: domains; system components and sub-components; and connections to other internal and external IT systems.

  A "domain" is a physically or logically contiguous region of an IT system, within which the environmental characteristics are uniform. It can be a definable boundary within a system in which (part or all of) a set of functions is executed; it can also include all or part of a network.

- The logical system boundary should include: interfaces with other internal IT systems; the information assets that flow between the IT system to other internal IT systems,

and through connections to external IT systems; the methods of transporting these flows; and the end sources (that is, where information originates, as well as its final destination).

A picture (diagram, architectural drawing, topology, etc.) might provide the best description of the IT system within the boundary of the analysis. For example, a diagram could show a mainframe or mini computer connected to a server, which is connected through Ethernet connections to PCs, printers, etc.

The list of assets provided in Annex F should assist in the identification of the major components within each boundary.

1.4 Choose the analysis team.

The number of team members will depend on the size and complexity of the IT system, as well as on the proposed scope and boundary of the analysis. Generally, TRA projects do not require more than three team members, plus an occasional resource person with subject-specific knowledge.

If the magnitude of the TRA is such that it should be conducted by a number of people as a team, each team member should have a vested interest in: the IT system; the business function; the data being processed; or the applications used to process the data. (Knowing something about, for example, the business process or the IT infrastructure supporting the process makes it easier to pinpoint vulnerable areas.)

1.4.1 Identify and recruit the team members who will perform the analysis.

Besides the TRA coordinator responsible for the project, team members might include departmental security officials (personnel, physical, Informatics, etc.); representatives from different levels of management; IT system administrators; and/or administrators and users who work directly with the applications.

1.4.2 Familiarize the team members with their requirements, and assign duties.

Team members should know why they are included on the team, and what contributions are expected of them. The more they know before work starts the less confusion there will be, and the easier it will be for them to work together.

1.5 Produce a Preliminary Statement of Sensitivity.

In order to implement appropriate security safeguards, it is essential to know what critical information and assets exist, and their sensitivity levels. This is accomplished by producing a Preliminary Statement of Sensitivity (SoS).

The production of an SoS is discussed in Annex D.

The Preliminary SoS should concisely identify at a very high level which assets need to be protected, along with their sensitivity levels.

Note: It is good practice to have an SoS for each business process being performed on an IT system.

1.5.1 Establish a target level (maximum level) of acceptable risk.

Although not essential at this point, it might be beneficial to estimate the maximum acceptable level of risk, as a guide for the analysis that is to follow.

Note 1: The target level of risk will have to be precisely defined in order to complete the recommendations in the final Risk Analysis Report.

Note 2: Establishing the maximum acceptable level of risk might have to wait until the assessment of system risks for acceptability is carried out during Task 8, when a better understanding of the risks to the system has evolved.

1.6 Collect information for the IT system description.

This should include descriptions of all physical and logical components that have been identified as being within the boundary of the analysis. They should describe:

- the IT system architecture
- information flows
- operational uses
- future plans
- the physical environment in which the IT system operates.

The required documents should be obtainable from operations-support personnel and/or managers. The information available will depend on when the TRA is being done within the IT system's life cycle: for an IT system under development, available information may be limited; whereas for an existing IT system, detailed information should be available. Note that in some instances, future plans may be included in a description of the system architecture.

Specific documents that might be collected include:

- an existing Statement of Sensitivity
- a previously conducted TRA
- descriptions of the system architecture

- descriptions of the applications processed on the system
- corporate security policies and standards
- a disaster recovery plan
- an organization chart
- diagrams (hardware floor plans, networks, site locations, security zones, etc.)
- service level agreements
- Royal Canadian Mounted Police (RCMP) SEIT reports.

Note: System diagrams that show hardware locations and information flows (including the end sources of information) should be collected whenever possible.

Refer to Annex B for an example of a typical IT system architecture description.

1.6.1 Create a list of the documents as they are collected.

For each document, include: title; source; and date received.

The list should be included as reference material in an annex of the final report. (The list can also serve as an audit trail, to show when and from whom each document was received.)

The list will need to be updated as more reference material is collected during the TRA.

1.6.2 Review the list of documents for completeness, and obtain missing documents.

It is important to identify out-of-date or missing documents and information, since much of the TRA process depends on reviewing accurate documentation. The focus and the results of the analysis can be greatly affected if current documents are not available for review. (Such omissions might also indicate problems in procedure or management.)

Senior technical personnel in operations should be able to provide missing information (diagrams, hardware, firmware, software versions, etc.). If not, the scope of the TRA must be reviewed, and the TRA might have to be halted until the situation is corrected. (Site visits, audits, penetration testing, and similar activities might be required in the absence of proper documentation.)

1.6.3 Review all documents collected in order to identify any components of the IT system that might have been missed, but that should be included within the boundary of the analysis.

1.6.4 Revise the boundary as required.

1.7 Collect existing descriptions of the organization.

Most (if not all) of this information can be obtained from an organization chart and its associated documentation, which are usually available from the human resources section of the organization.

Collect descriptions of:

- the organizational structure
- the reporting structure
- reporting relationships
- responsibilities
- authorities.

1.7.1 Include these documents on the list created in Step 1.6.1.

1.7.2 Identify and record key personnel positions.

Review the documents collected to identify key positions in the operation of the IT system, and record any that might provide additional information for the analysis.

This should include the management, operational and technical positions among the managers and the users of the system. These are the positions of asset owners who will be instrumental in identifying and assigning value to assets during Task 2.

1.7.3 Create a list of personnel.

Create a list of the personnel holding the key positions identified in Step 1.7.2. Include:

- job title
- office location
- e-mail address
- telephone and fax numbers.

This list will be required during the preliminary analysis of the work plan. The list should also be included as reference material in an annex of the final report.

1.8 Formulate a system description.

Review the information collected in Steps 1.6 and 1.7, and produce a system description. (Refer to Annex B.)

Record the IT system's:

- elements
- concept of operations
- mode of operation.

Also include a user profile, and the impact of planned changes.

Explanations regarding mode of operation and concept of operation can be found in the glossary at Annex K.

Note: In the case of a new or proposed system, the concept of operations is fundamental to the development of the requirements of the IT system.

1.9 Devise a work plan.

1.9.1 Review (and revise if required): the team members selected in Step 1.4; and their assigned duties.

1.9.2 Review the organizational and management information collected in Step 1.7.

Record the critical:

- organizational issues;
- responsibilities; and
- reporting relationships,

as they will guide the focus of the analysis.

1.9.3 Review the system description formulated in Step 1.8.

Record the critical:

- information flows;
- procedures; and
- associated practices,

as this will help identify critical assets.

1.9.4 Develop questionnaires for the interviews of key personnel.

Interviews based on questionnaires are useful for identifying assets, determining asset values, and correcting missing or out-of-date information. The Preliminary SoS produced in Step 1.5 identifies which assets the questionnaires should focus on to get this information.

Note: An existing SoS might be used to obtain asset values. The TRA process should **not** proceed, however, unless a current SoS has been developed and approved by senior management.

Elements to consider when designing a questionnaire include:

- impact on the organization if the IT system is unavailable
- the user community (who has access to the system and at what level)
- connections to other systems (both internal and external to the organization)
- confidentiality requirements
- integrity requirements
- availability requirements
- security procedures

- personnel-training and security-awareness issues.

Refer to Annex C for a sample questionnaire.

1.9.5 Identify personnel to receive questionnaires.

From the key personnel listed in Step 1.7.3, identify and record the management, operational and technical personnel who will be instrumental in identifying and assigning value to assets.

Also record which interviews will require site visits (it might be sufficient in some instances to conduct interviews by telephone), and the type of information that is expected from each interview.

Revise the list as required.

1.9.6 Estimate the time required to perform site visits and interviews.

Allow one hour to prepare for each interview, one hour (or less) to conduct the interview, and one hour to review and record the information collected at the interview.

If travel time is required, it is a good idea to limit the number of interviews to two (or a maximum of three) per day.

The time required for site visits to operations processing centres/offices will depend on the size of the IT system; the recommendations listed in RCMP SEIT reports (if available) on these sites should form a good basis for determining the amount of information required.

1.10 Review and revise the work plan as required.

TASK 2 – COLLECT DATA FOR ANALYSIS

(Document produced: Initial Security Review)

2.1 Collect information about threat agents, threat events and vulnerabilities.

This information should provide insight into which assets are at the greatest risk from threat agents. It is important that this information be properly interpreted, with some indication of its relative importance to the analysis.

Note: Consider the sensitivity of this information, as it might be sensitive corporate information that must be treated as Protected B, Secret or higher.

2.1.1 Identify sources of information about threat agents, threat events and vulnerabilities.

Historical information should be available from the DSO, and from equivalent security personnel at other Government departments and agencies. Additional information might also be available from Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), and the RCMP IT Security Branch.

Relevant information might also be found in the open literature (that is, in IT publications).

2.1.2 Create a contact list from the identified sources.

Include:

- job title
- department or agency
- location
- telephone and fax numbers
- e-mail address
- date contacted.

This list should be included in an annex of the final report.

2.1.3 Contact the identified sources, and collect available information on threat agents, threat events and vulnerabilities.

Include the documents containing this information (and their sources) on the list created in Step 1.6.1.

Note: Accuracy is essential, since this information will be used in Tasks 5 and 6.

2.2 Distribute questionnaires; conduct interviews and site visits.

2.2.1 Contact the key personnel identified in Step 1.9.5 to arrange delivery of the

questionnaires developed in Step 1.9.4, and to schedule the subsequent interviews.

It is worthwhile to explain the rationale behind the questionnaire, and the value of the interviewee's contribution to the TRA process.

2.2.2 Distribute the questionnaires.

This should be done far enough in advance of the interviews to allow the interviewees adequate preparation time. Delivery should be by the fastest method (fax, e-mail, etc.) that is convenient for the interviewee.

Where applicable, a sample list of assets (see Annex F) might be attached to the questionnaire.

2.2.3 Interview the key personnel.

After each interview, review and record the information collected. Notes from the interview should be transcribed as soon as possible after the interview, while memories are still fresh.

2.2.4 Conduct the site visits.

After each site visit, review and record the information collected. Notes from the site visit should be transcribed as soon as possible after the site visit, while memories are still fresh.

2.2.5 Review the information collected during the interviews and the site visits, and carry out any follow-up interviews that might be required.

In most instances follow-up interviews can be conducted by telephone, as the information required is usually for the clarification of specific details, or to reconcile differing responses from multiple sources.

2.3 Review the questionnaires and the notes from the interviews, in order to identify sensitive assets.

Sensitive assets are those assets that are most likely to be at risk from threat agents.

2.3.1 Record the sensitive assets in terms of the categories provided in Annex F.

Note: The asset list might be only partially complete, depending on when the assessment is performed during the IT system's life cycle.

2.4 Review the information collected to this point, and record the existing security architecture in the Initial Security Review.

Information in the Initial Security Review will be used during Tasks 5 and 6.

Note: The assistance of DSO support staff is required to complete Step 2.4.

2.4.1 Record the concept of operations.

This was described in the System Description formulated in Step 1.8.

2.4.2 Record the existing policy framework.

This information was collected during Step 1.2.3.

2.4.3 Record the existing physical security measures.

This information was collected during the interviews, from available RCMP SEIT reports, and in Step 1.6.

2.4.4 Record the existing personnel security measures.

This information was collected during the interviews, from available RCMP SEIT reports, and in Step 1.6.

2.4.5 Record the existing procedural and operational security measures.

This information was collected during the interviews, from available RCMP SEIT reports, and in Step 1.6.

2.4.6 Record the existing computer security measures for stand-alone systems.

This information was collected during the interviews, from available RCMP SEIT reports, and in Step 1.6.

2.4.7 Record the existing network security measures.

This information was collected during the interviews, from available RCMP SEIT reports, and in Step 1.6.

Network security includes operational policy and procedures, administrative responsibilities, and issues related to connections between systems handling different security levels. At the operational level, it includes:

- transmission security: operational procedures and controls, and methods to prevent interception, exploitation and deception during internal and external transmission of data over networks;
- cryptographic security: communications security procedures and practices for the transmission of highly sensitive data over networks, as well as cryptographic key management;
- emission security: the interception and analysis of emissions during the transmission and/or processing of data; and
- telecommunications security: measures designed to protect data during storage, transmission and/or processing.

2.4.8 Record any existing security level-of-awareness training plans.

This information was collected during the interviews.

TASK 3 – ANALYSE POLICY AND STANDARDS COMPLIANCE

(Document produced: List of Non-Compliant Areas)

Departmental policies and standards are the rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within the organization and its IT systems.

It is essential that any non-compliant areas of the IT system be identified and recorded, so that they can be assessed during Tasks 5 and 6.

3.1 Identify applicable security policies and standards concerning departmental IT systems.

This information was collected during Step 1.2.3, and incorporated into the Initial Security Review in Step 2.4.

3.2 Review the system description formulated in Step 1.8 with regard to the applicable security policies and standards, and record any system deficiencies in the List of Non-Compliant Areas.

3.3 Identify and record existing/planned safeguards.

The policy and standards documents collected in Step 1.2.3 should note the existing and planned safeguards for reducing risk. Identify and record them in a format convenient for later use; existing/planned safeguards might help satisfy the requirements for protection of non-compliant areas during Task 8.

TASK 4 – PERFORM AN ASSET SENSITIVITY ANALYSIS

(Document produced: Statement of Sensitivity Report)

Refer to the Preliminary SoS produced in Step 1.5. If a detailed analysis of the IT system is called for, the Preliminary SoS should be used to focus the work in this task.

Note: In instances where a detailed analysis is **not** required, the TRA assessment process can eliminate Steps 4 to 7, and proceed directly from Task 3 to Task 8.

A "valuation of IT assets" represents the importance of IT assets to the business of an organization, by identifying and assigning value to those assets. Valuing the assets allows the analyst to decide which IT areas are the highest priority, and consequently where security efforts should be focused.

4.1 Identify and record the system domains.

The IT system domains were defined in Steps 1.3 and 1.8. At a high level, these will probably be representative of business functions being performed (in business units such as accounts payable, research and development, payroll and personnel).

Note: In some instances, the domains might represent multiple security zones.

4.2 Put the domains in order for assessment.

Care must be taken to ensure that areas of primary concern or sensitivity are assessed first. (Also, since safeguards adequate for highly sensitive domains usually protect less-sensitive domains, it will save effort to order the domains by degree of sensitivity.)

4.3 Analyse asset sensitivities within each domain.

Analyse each domain in the sequence chosen in Step 4.2.

Within the domain being analysed, rate the sensitivity of each asset according to the asset sensitivity rating scale (Table II) in Annex A. Rate the sensitivity in terms of:

- confidentiality
- integrity
- availability
- replacement value.

The analysis of any one asset with regard to confidentiality, integrity, availability and replacement value should be done at the same time (in parallel).

Keep in mind that an asset's sensitivity in terms of confidentiality, integrity and availability can be measured both qualitatively (in relative terms) as well as quantitatively (in terms of dollar losses). Qualitative and quantitative elements should be considered together when assessing asset

sensitivity.

Furthermore, when assessing sensitivity the analysts(s) should consider the loss of prestige, trust or business opportunity (that is, the impact on intangible assets) that would result: from the violation of confidentiality, integrity or availability; or due to the cost of replacement.

4.3.1 For each asset within the domain, assess and record the sensitivity in terms of confidentiality.

This is the impact on the IT system and/or the organization that would result from the deliberate, unauthorized or inadvertent disclosure of the asset.

Note: This assessment requires that the asset owner has clearly defined the confidentiality level of the asset.

4.3.2 For each asset within the domain, assess and record the sensitivity in terms of integrity.

This is the impact on the IT system and/or the organization that would result from the deliberate, unauthorized or inadvertent modification of the asset.

Note: This assessment requires that the asset owner has clearly defined the integrity level of the asset.

4.3.3 For each asset within the domain, assess and record the sensitivity in terms of availability.

This is the impact on the IT system and/or the organization that would result from the deliberate or accidental denial of the asset's use.

Note: This assessment requires that the asset owner has clearly defined the maximum acceptable time that each asset may be unavailable.

4.3.4 For each asset within the domain, assess and record the sensitivity in terms of replacement value.

This is the total financial impact on the organization that would result from the physical loss or destruction of the asset.

Note: This assessment requires that the asset owner has defined the replacement value of the asset.

4.3.5 Review the assessments with the asset owners, and revise as needed.

4.3.6 Repeat Steps 4.3.1 to 4.3.5 for each domain, until the assets in all domains have been assessed.

4.4 Summarize asset sensitivities.

Summarize the asset sensitivities, by identifying the highest-sensitivity-level asset categories in each domain.

4.5 Evaluate the Preliminary Statement of Sensitivity.

After assets have been rated in terms of confidentiality, integrity, availability and replacement value, a comparison needs to be made to the Preliminary SoS prepared in Step 1.5.

4.5.1 Reconcile any anomalies between the Preliminary SoS and the assessments carried out during Task 4.

This should result in a true picture of the sensitivity of the assets.

4.6 Identify those assets deemed to be the most sensitive or critical to the business process, in the Statement of Sensitivity Report.

The identified assets should be selected for analysis in Tasks 5, 6 and 7.

TASK 5 – PERFORM A THREAT ANALYSIS

(Document produced: Threat Analysis Report)

Note: The threat analysis (Task 5) and the vulnerability analysis (Task 6) should be performed in whichever order will simplify and expedite the risk analysis (Task 7) of each IT system. It might make more sense to look at threats and threat agents first, or to look at vulnerabilities first. As long as *all* possibilities are considered (even if only to dismiss them), the order of consideration is not crucial.

5.1 Identify potential threat agents for each domain.

Refer to the Sample List of Threat Agents (Annex G), and to the information recorded in Step 2.1. Select those threat agents that could act upon the assets that were identified as most sensitive in Task 4.

Note: As technology is continually evolving, new threat agents might appear that are not included in Annex G. If this happens, amend Annex G accordingly.

5.2 Identify the potential threat events by which threat agents could compromise the assets within each domain.

Threat events are the actions by which threat agents attack assets. (Threat events can be active [modifying or destroying, etc.] or passive [eavesdropping, looking in garbage, etc.].)

Using the Sample List of Threat Agents (Annex G), the Sample List of Threat Events (Annex H), and the information recorded in Step 2.1, identify the threat events by which threat agents could compromise each of the most sensitive or critical assets identified in Task 4.

The analysis should include both accidental and deliberate threat events.

Note: New threat events might appear that are not included in Annex H. If this happens, amend Annex H accordingly.

5.3 For each potential threat event, analyse its threat agents in terms of capability and motivation.

This is accomplished by working through the threat agent rating tables (Tables III, IV and V) in Annex A, for each threat agent.

5.4 Analyse the likelihood of each potential threat event occurring.

Likelihood can be expressed:

- in terms of frequency of occurrence;
- by annualized frequency; or
- in qualitative terms,

as appropriate.

The information necessary to make this analysis was collected and collated during Task 2.

5.5 Summarize the threat analyses individually for each domain.

For each asset within the domain, identify those threat events that have a high likelihood of occurring.

5.6 Record the threat analysis summaries in the Threat Analysis Report

Record the potential threat events identified in Step 5.5 by domain, according to the highest-level asset categories (as defined in Annex F) that are at risk.

TASK 6 – PERFORM A VULNERABILITY ANALYSIS

(Document produced: Vulnerability Analysis Report)

6.1 Identify the vulnerabilities that could cause harm to individual assets within each domain.

Refer to the Sample List of Vulnerabilities (Annex I), the system description recorded in Step 1.8, and the information collected in Step 2.1.

6.2 For each vulnerability, rate the likelihood of that vulnerability being exploited.

This is accomplished by working through the vulnerability rating tables (Tables VI, VII and VIII) in Annex A.

6.2.1 Rate the exposure level of the vulnerability

Use Table VI to rate the exposure level of the vulnerability. Take into consideration the potential effects in terms of:

- disclosure;
- modification; and
- denial of service (including through interruption, destruction or removal).

6.2.2 Rate the severity level of the vulnerability.

Use Table VI to rate the severity level of the vulnerability. Take into consideration the potential effects in terms of:

- confidentiality;
- integrity; and
- availability.

6.2.3 Determine the overall rating of the vulnerability.

Use Tables VII and VIII to determine the overall rating of the vulnerability.

6.2.4 Identify any safeguards already in place that would reduce the severity of an attack exploiting the vulnerability.

6.3 Produce the Vulnerability Analysis Report.

Summarize the vulnerability analysis, in the Vulnerability Analysis Report.

6.3.1 For each domain, record the vulnerabilities with the highest exposure and severity ratings, as well as the vulnerabilities with the highest overall ratings.

6.3.2 For each domain, record the vulnerabilities according to the highest-level asset categories (as defined in Annex F) that are at risk.

6.3.3 Record which safeguards already in place protect particular assets from the recorded vulnerabilities.

TASK 7 – PERFORM A RISK ANALYSIS

(Document produced: Risk Analysis Report)

A risk analysis attempts to analyse all potential major threat events, and their associated consequences.

7.1 Identify possible threat scenarios.

7.1.1 Review the Threat Analysis Report along with the Vulnerability Analysis Report, in order to identify possible threat scenarios.

A threat scenario consists of one or more threat events, carried out by a threat agent, that could result in the compromise of an asset.

Analyse each potential threat event identified in Task 5 with respect to the safeguards identified in Task 6, in order to determine how effectively the existing safeguards will protect particular assets from threat agents (or, in other words, the likelihood of threat agents producing harm to, or loss of, the assets). Include the estimated frequency of occurrence.

7.1.2 Identify the threat scenarios that make logical sense.

Provide the rationale for discarding any threat scenario.

7.2 Analyse the resulting risk in each domain.

7.2.1 Estimate the likelihood of each logical threat scenario occurring.

Base the estimate on the likelihood of: 1) the threat agent acting (considering both capability and motivation) to take advantage of a vulnerability; or 2) the natural phenomenon occurring.

7.2.2 Analyse the potential impact on the IT system and/or the organization of each logical threat scenario.

Take into consideration asset sensitivity, and the vulnerability rating determined in Step 6.2.3.

7.2.3 Assess the level of risk from each logical threat scenario.

Consider the likelihood of occurrence in conjunction with the potential impact on the IT system and/or the organization.

Note: This is not necessarily represented by a simple algebraic relationship. For example, there might be a potential threat scenario with such grave consequences that even one occurrence would be intolerable.

7.3 Produce the Risk Analysis Report.

Summarize the risks, in the Risk Analysis Report.

Note: Since adequate protection should lead to low likelihood of a threat scenario occurring, areas that have adequate protection will **not** emerge as needing protection. Areas that have inadequate protection **will** emerge as needing protection.

7.3.1 For each domain, select and record the risks having the highest potential impacts within the domain.

7.3.2 Summarize the risks within each domain.

Record the highest-level asset categories (as defined in Annex F) that would be at risk from the identified threat scenarios.

7.3.3 Select and record, from all domains, the risks with the highest potential impacts for the overall system.

7.3.4 Summarize the risks for the overall IT system.

Record the highest-level asset categories (as defined in Annex F) that would be at risk from the identified threat scenarios.

TASK 8 – ASSESS SYSTEM RISKS FOR ACCEPTABILITY

(Document produced: Preliminary Risk Assessment Report)

This assessment should indicate the degree of risk associated with the IT system's defined assets.

The results are important, because they are the basis for selecting the safeguards necessary to protect the assets, accomplished by comparing alternatives until an acceptable safeguard (or combination of safeguards) can be selected.

Note: The selection of safeguards that are appropriate, are affordable, and provide minimal impact on productivity might require the judgment of a security professional. (For example, in order to reduce opportunities for theft, it might require the assistance of the RCMP, departmental legal staff, and/or other experts.)

8.1 Meet with the Project Authority to confirm the maximum acceptable level of risk.

Review the completed assessments, and confirm the maximum level of residual risk that will be acceptable after safeguards are implemented. (If an estimated level of acceptable risk was established in Step 1.5.1, review and revise it with the Project Authority.)

These risk-acceptance decisions will be factored into the selection of safeguards.

8.2 Review the system risks identified in Task 7, for validity and Sensibility.

Confirm that the IT system could be reasonably considered to be at risk from the recorded threat scenarios.

8.3 Review the existing/planned safeguards.

These are the protection mechanisms that were identified and recorded in Step 3.3.

8.4 Assess whether or not existing/planned safeguards provide adequate protection.

8.4.1 Identify any vulnerabilities.

If no safeguard is providing adequate protection, it can be assumed that there is a vulnerability.

8.4.2 Ensure that one or more of the existing/planned safeguards addresses each newly identified vulnerability.

8.4.3 Record any vulnerabilities that are not addressed by the existing/planned

safeguards.

These will need to be included in the Risk Assessment Report.

8.5 Assess whether or not all of the existing/planned safeguards are required.

An existing or planned safeguard might not be required, if another safeguard adequately protects an asset.

Note: Overprotection can be costly, and can add to operational overhead.

8.6 Select additional safeguards for possible implementation.

When selecting safeguards for implementation, a number of factors should be considered, including:

- the safeguard function(s) performed (see below)
- relative strength of the safeguard
- ease of use
- transparency to the user
- the help available to the user when performing safeguard functions.

Safeguards can be divided into eight categories, according to the specific functions by which they protect assets. (Many safeguards perform functions from multiple categories; they tend to be the preferred safeguards.)

The safeguard function categories are:

- **Correction:** Implementing a safeguard to mitigate a known vulnerability
- **Detection:** Detecting the source of a threat
- **Deterrence:** Discouraging threat agent activity
- **Prevention, or Avoidance:** Changing operations to prevent threat agent activity (for example, by removing Internet access from a network and then using a standalone PC for Internet access)
- **Containment:** Limiting the injury/loss that a successful threat event could cause (for example, by having a Business Resumption Plan)
- **Recovery:** Providing the ability to quickly recover an IT system from a successful threat event, to its original (or at least to a degraded but usable) state

- **Monitoring:** Monitoring an IT system for vulnerabilities and/or for threat agent activities
- **Awareness:** Informing personnel about security issues through well-regulated security awareness programs.

8.6.1 Select a safeguard (or a combination of safeguards) that will effectively protect each category of IT system assets.

Less sensitive, less essential assets will require minimal safeguards, while highly sensitive or critical assets will merit much stricter protective measures.

8.6.2 Identify the residual risk that would remain for each safeguard if it were selected for implementation.

8.6.3 Assess the selected safeguards for acceptability.

Acceptability depends upon: the current security situation; accepted business practices; cost-effectiveness; tolerable loss threshold; and any other standards that are appropriate under the circumstances.

Also consider possible constraints, as they might affect the selection of safeguards. Some constraints to consider are:

- legal constraints
- contractual constraints (lease agreements, etc.)
- collective agreements
- cost
- potential loss of productivity
- operational overhead
- enforceability
- management style.

8.7 Revise until acceptable safeguards can be recommended.

Review the results and repeat Steps 8.1 to 8.6 as needed, until the chosen safeguards provide an acceptable level of residual risk for each category of IT system asset.

8.8 Produce the Preliminary Risk Assessment Report.

Record the acceptable safeguards, and recommend the preferred safeguards, in the Preliminary Risk Assessment Report.

TASK 9 –DELIVER THE FINAL RISK ASSESSMENT REPORT

(Document produced: Final Risk Assessment Report)

9.1 Prepare the Final Risk Assessment Report.

This report assembles all of the reports and annexes created during the project. These include:

- Work Plan
- System Description
- Preliminary Statement of Sensitivity
- Initial Security Review
- List of Non-Compliant Areas
- Statement of Sensitivity Report
- Threat Analysis Report
- Vulnerability Analysis Report
- Risk Analysis Report
- Preliminary Risk Assessment Report
- Final Risk Assessment Report.

9.2 Present the Final Risk Assessment Report.

Present the report to the Project Authority, for further presentation to the Designated Approving Authority.

ANNEX A – Rating Tables

Asset Sensitivity Rating

A critical step in the TRA process is the completion of a Statement of Sensitivity (SoS) in order to determine the confidentiality, integrity, and availability requirements of the assets.

An SoS covers many components, including:

- the type(s) of information processed through the system;
- the information's value to the organization or department;
- the application(s) (and code) through which the information is processed;
- the equipment on which applications are resident; and
- the personnel who operate, administer, and manage these elements.

A general rating system can be employed to determine the levels of sensitivity of each asset's confidentiality, integrity, and availability requirements. Such a rating system is provided within this annex.

Note: The rating scales in this annex (Annex A) rank several *dimensions of risk*. The numbers are **not** related to the numbers representing *levels of detail* in Annexes F through I, and should **not** be confused with them.

Table II - Asset Sensitivity Rating Scale

Rating	Description
1	Breach could result in little or no loss or injury.
2	Breach could result in minor loss or injury.
3	Breach could result in serious loss or injury, and the business process could be negatively affected.
4	Breach could result in very serious loss or injury, and the business process could fail.
5	Breach could result in high-dollar losses, or in exceptionally grave injury to an individual's or the organization's: well-being; reputation; privacy; or competitive position, and the business process will fail.

Threat Agent Rating

Threat agents are those entities that could (deliberately or unintentionally) exploit vulnerabilities to harm assets.

Threat agents are rated in terms of motivation and capability.

- "Motivation" is a measure combining the potential benefit to the threat agent, and the resources available to the threat agent.

  Note: Motivation is not a factor for natural or other randomly occurring phenomena.

- "Capability" is a measure of a threat agent's ability (including the level of effort required) to successfully attack an asset by exploiting its vulnerabilities.

  Capability can be further broken down into:
  - technical ability
  - knowledge
  - resources
  - opportunity.

Table III - Threat Agent Capability and Motivation Ratings

Capability	Rating	Motivation
Little or no capability to mount an attack.	**1**	Little or no motivation. Not inclined to act.
Moderate capability. Has knowledge, skills to mount attack, lacking in some resources. Or, lacking some knowledge but has sufficient resources to mount an attack.	**2**	Moderate level of motivation. Would act if prompted, or provoked.
Highly capable. Has knowledge, skills and resources to mount an attack.	**3**	Highly motivated. Almost certain to attempt an attack.

Table IV - Threat Agent Rating Combinations

Capability Rating	Motivation Rating		
	1	**2**	**3**
1	1	2	3
2	2	3	4
3	3	4	5

Table V – Overall Threat Agent Ratings

Rating	Description
1	Little or no capability or motivation.
2	Little or no capability, moderate level of motivation. Or, moderate capability, little or no motivation.
3	Highly capable, little or no motivation. Or, little or no capability, highly motivated. Or, moderate capability, moderate level of motivation.
4	Highly capable, moderate level of motivation. Or, moderate capability, highly motivated.
5	Highly capable, highly motivated.

Vulnerability Rating

The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or a set of conditions that could allow assets to be harmed by an attack.

A vulnerability is rated in terms of:

- the severity of impact; and
- the potential exposure to loss,

resulting from the occurrence of one or more threat events.

Table VI - Vulnerability Severity and Exposure Ratings

Severity	Rating	Exposure
Minor severity: Vulnerability requires significant resources to exploit, with little potential for loss.	**1**	**Minor exposure:** Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited.
Moderate severity: Vulnerability requires significant resources to exploit, with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	**2**	**Moderate exposure:** Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High severity: Vulnerability requires few resources to exploit, with significant potential for loss.	**3**	**High exposure:** Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.

Table VII - Vulnerability Rating Combinations

Severity Rating	**Exposure Rating**		
	1	**2**	**3**
1	1	2	3
2	2	3	4
3	3	4	5

Table VIII – Overall Vulnerability Ratings

Rating	**Description**
1	Minor exposure, minor severity.
2	Minor exposure, moderate severity; or moderate exposure, minor severity.
3	Highly exposed, minor severity; or minor exposure, high severity; or moderate exposure, moderate severity.
4	Highly exposed, moderate severity; or, moderate exposure, high severity.
5	Highly exposed, high severity.

ANNEX B – Sample Description of a Typical IT System Architecture

B.1 Contents

An IT system description includes (with applicable diagrams, if available):

- the concept of operations of the system (see B.2, below)
- the mode of operation of the system (see B.3, below)
- identification of the physical site locations (including any disaster recovery sites)
- identification of the different security zones at each site (including all rooms that contain components of the IT system within each security zone)
- identification of the hardware at each location (mainframe, mini, servers, etc.)
- descriptions of the applications used, and the security level(s) of the information handled on the system
- identification of the types of users of the system
- identification of all internal and external network connections, as defined by the system boundary
- identification of any factors, within the physical environment in which the IT system operates, that might have an impact on the system (including such factors as temperature, humidity, dust and power outage)
- any plans for changes to the IT system.

B.2 Concept of Operations

A concept of operations identifies an IT system's:

- purpose
- size
- functional characteristics.

The *functional characteristics* of an IT system include:

- the type(s) of information handled
- the type(s) of application(s) supported/type(s) of processing carried out
- user groups
- the connectivity between functions
- the connectivity to the external world, as defined by the system boundary
- the system's expected performance requirements.

B.3 Mode of Operation

A mode of operation categorizes an IT system with respect to the controls that are needed to enforce security policy requirements based on security clearance/screening, and the need-to-know. The GSP defines three possible modes of operation for Government of Canada systems:

- **Dedicated: All** users have the need-to-know regarding **all** of the information on the system, and **are cleared** to access **all** of the information on the system
- **System high: All** users have the need-to-know regarding **some** of the information on the system, but nevertheless **are cleared** to access **all** of the information on the system
- **Multilevel: Some** users have the need-to-know regarding **some** of the information on the system, and **are not cleared** to access **all** of the information on the system (that is, they are cleared to access only some of the information on the system).

  Note: An IT system might be assumed to be a multilevel system if it permits multiple security classification levels of data to be concurrently stored and processed.

The Department of National Defence (DND) divides multilevel-mode IT systems into two less permissive subsets:

- **Compartmented: All** users have the need-to-know regarding **some** of the information on the system, and are permitted access to **some** of the information on the system, although they are cleared to the highest security classification level of the information on the system.

  Note: An IT system in this mode is operated only in a closed environment.

- **Controlled:** The IT system places constraints on an entity (end user, etc.) attempting to make a connection.

  Note 1: An IT system in controlled mode is operated only within a closed environment.

  .

  Note 2: An IT system might be assumed to be a controlled system if the likelihood of threat agents accessing the system from an external system is very low.

ANNEX C – Sample Questionnaire

Adapted from: Annex B of CSE publication *A Trusted Systems Environment Guidelines (CID/09/17)*

This questionnaire is included as a guide for the preparation step of a TRA and may need to be modified to suit the analysis requirements for each IT system. Completion of the questionnaire is **vital** as all following TRA steps draw on this information as input.

Completion of the questionnaire will help to clarify details of the IT system, and will facilitate the consultation process with the management, operational, and technical personnel who will be instrumental in identifying and assigning value to assets. For questions that can be answered with "yes", give details.

A diagram of the system architecture and a sample taxonomy of assets may be included to assist those with the task of answering the questions.

Selection of a Mode of Operation for the system, the final part of the preparation step, is discussed in the text.

Note: This general form of the questionnaire is applicable to both existing and new systems. However, for new systems some of the answers necessarily will be for the system as foreseen, and some may be unanswerable (e.g.,: choice of hardware, security features in place) on the first few passes through what is recognized to be an iterative process. See the discussion in the text.

System Description

Purpose:

1. Who are the user groups of this system? (Depending on the size of the system they may be organizations and/or their agencies, departmental divisions/sections, etc.)
2. What is the function of the system?
3. What does the system deliver?
4. What is the impact on the organization if the system is destroyed or unavailable for a long period of time?

Functional Characteristics: Applications

1. What processes are carried out by the applications on the system? (e.g.: database, electronic mail, personnel information, word processing, program development)

Functional Characteristics: Configuration

1. What hardware does the system use?
2. What operating system software does the system use? (e.g.: Novell, NT, Banyon, etc.)
3. What operating system security features are being used?
4. What system security features are available? (e.g.: use of trusted system, add-on security packages)

Functional Characteristics: Communications

1. Does this system have external connections? (e.g.: LAN, Internet, dial-in, dedicated lines). If so, describe each.
2. What communications security features are in use? (e.g.: dial-back modems, encryption, dedicated lines)

Statement of Sensitivity

Primary Risk Factors

1. What is the maximum level of sensitivity of the information to be processed on the system? The departmental classification guide should be used in replying to this question.

2. What is the minimum user screening level?
   a. Unscreened unsupervised;
   b. Unscreened supervised;
   c. Basic reliability check;
   d. Enhanced reliability check;
   e. Level I clearance;
   f. Level II clearance; and
   g. Level III clearance.

3. What Mode of Operation will the system operate under?
   a. Dedicated;
   b. System High; and
   c. Multilevel.

Other Factors

Nature of the Information

1. Are there requirements to strictly limit access by users to any part of the information held (e.g.: information restricted to only those who have a “need-to-know”)? If yes, give details.

2. Are there requirements to separate information among users on the system (e.g.: information for which the user has the appropriate screening or clearance level, but does not require in his/her duties)? If yes, give details.

3. What quantity of information is held (e.g.: by number of records, bytes of storage, disks, etc.; storage requirements should be available in the Disaster Recovery Plan)?

4. Are there concerns for aggregation or context such that the whole of the information held warrants a higher classification than any individual record? If yes, give details.

5. Identify the proportion of sensitive information at each level, for example as:
   a. _____% unclassified;
   b. _____% Sensitive (Protected A);
   c. _____% Particularly Sensitive (Protected B);
   e. _____% Extremely Sensitive (Protected C);
   e. _____% Confidential;
   f. _____% Secret; and
   g. _____% Top Secret.

6. Will the information be downgraded in sensitivity in the near future? If yes, give details.

7. Identify how the sensitive information is stored and the proportion for each, for example on:
   a. _____% paper;
   b. _____% hard disks;
   c. _____% cartridges;
   d. _____% tapes; and
   e. _____% floppies.

8. Identify the methods of disposal for assets used for sensitive information (e.g.: paper, hard disks, cartridges, tapes, floppies, etc.).

User Community

1. How many users are there on the system?

2. What is the distribution of users by security screening (you may want to differentiate users, operators, programmers, administrators, privileged users etc.)? This might be expressed as:
   a. _____% unscreened unsupervised;
   b. _____% unscreened supervised;
   c. _____% basic reliability check;
   d. _____% enhanced reliability check;
   e. _____% level I clearance;

f. _____% level II clearance; and
g. _____% level III clearance.

3. What are the characteristics and level of expertise among those accessing the system? This might be expressed as:
   a. _____% user only;
   b. _____% programmer;
   c. _____% operations;
   d. _____% privileged users; and
   e. _____% systems administrators.

4. Where are the users located? Describe physical security measures available at each location.

5. What types of terminals are involved?
   a. limited function;
   b. "dumb" terminal;
   c. "intelligent" workstation or PC; and
   d. server.

System Attributes

1. How would you describe threats from outside of the system boundary (e.g.: from hackers, viruses, criminals, foreign governments, news media, etc.?
   a. hostile;
   b. neutral; and
   c. benign.

2. Are there aspects of the system architecture that would make it particularly vulnerable to the compromise of sensitive information?

3. What controls are in place for application development and testing?

4. Are there particular difficulties in the area of configuration management and change control? If yes, give details.

Requirements for Audit

1. Is there an audit trail of all user actions within the system? If so, describe what audits are done. (e.g.: in a database environment, it may be required to know who can read, write or modify which records. With NATO Secret material, there is a NATO requirement to audit any access to it.)

Confidentiality Requirements

1. What are the requirements for confidentiality (disclosure of information) in the system? How important is it that the information in your system be seen by only those who have a need-to-know? Describe the potential impact of disclosure of the information in your system.

Integrity Requirements

1. What are the requirements for integrity (correctness and completeness of information) in the system? How important is it that the information in your system be completely accurate? Describe the potential impact of corruption of the information in your system.

Availability Requirements

1. What are the requirements for availability (system functioning when needed)? This might be described in terms of:
   a. _____% recovery in 5 minutes
   b. _____% recovery in 1 hour
   c. _____% recovery in 1 day
   d. _____% recovery in 1 week
   e. _____% recovery in 1 month
   f. _____% recovery in _____

If applicable, which applications or portions of the system must be recovered at each stage?

ANNEX D – Contents of a Statement of Sensitivity

The sensitivity of an IT system, and the information processed, transmitted or stored on it, needs to be defined and recorded in a Statement of Sensitivity (SoS). An SoS provides direction for a TRA, and is essential as input for all following tasks in the TRA process.

Note: The analyst must consider several aspects that contribute to the worth of an asset in addition to the initial cost of the item; an asset can have an **acquired** value that far outweighs the initial cash outlay.

In addition, the **sensitivity-related** value of the asset is not necessarily linked to the numerical values associated with its initial or replacement cost, but rather is linked to the relative value that is associated with the asset's requirements regarding confidentiality, integrity and availability.

When producing an SoS:

1. Prepare a list of IT system assets (refer to Annex F), and record each asset at its highest level within each category that is part of the IT system.
2. Identify only the most critical IT system (and related) assets that need to be protected.
3. Record the value of each of these critical assets in terms of:
    - *confidentiality* (consider the loss or harm that would result from unauthorized disclosure of the asset, or of the information handled or protected by the asset);
    - *integrity* (consider the loss or harm that would result from unauthorized modification of the asset); and
    - *availability* (consider the loss or harm that would result from partial or total unavailability of the asset).

Try to limit the SoS to one page (or to a maximum of two pages for a complex system). (Note that the assets might have to be summarized at the highest category levels in order to achieve this.)

A sample form that can be used as the basis for recording the information that will be used in producing the SoS is provided on the following pages of this annex.

The assets in Annex F are grouped into the following categories.

- **Information:** Includes all data that is created, processed, transmitted, stored or managed within the IT system.
- **Processes:** Includes those elements that comprise the fundamental steps in creating, processing, transmitting, maintaining and reporting on information assets.
- **Platforms:** Includes the hardware elements of the IT system. (Note that confidentiality is not applicable to this category of assets for most IT systems.)
- **Interfaces:** Includes those elements that provide the capability to communicate between system components, or through the system boundary.
- **Personnel:** Includes any personnel who interact with the system. (Note that confidentiality and integrity are not applicable to this category of assets; availability is

the primary concern.)

- **Environment:** Includes the physical aspects of the site(s), including environmental controls. (Note that confidentiality is not applicable to this category of assets for most IT systems.)
- **Intangible:** Includes non-physical assets that are difficult to put a value on (for example, goodwill).

Adapted from RCMP SIP5 Document, APPENDIX B Page 1

SAMPLE STATEMENT OF SENSITIVITY

GENERAL INFORMATION

Branch:_____ Division:_____

Contact Name:_____ Phone:_____

Fax:_____ E-mail:_____

ENVIRONMENT:

(System)
System Name:_____

Application:_____

Other:_____

(Hardware)
Mainframe/Mini:_____

Micro Computer:_____

LAN/WAN/MAN:_____

Secure Phone/FAX:_____

Other:_____

CONFIDENTIALITY

Is the information processed considered:

CLASSIFIED ( ) No ( ) Yes Level (if Yes):_____
or
DESIGNATED ( ) No ( ) Yes Level (if Yes):_____
or
Can the information be released under the Access to Information statute?
( ) No ( ) Yes
Details:_____

What would be the consequences if data are disclosed to unauthorized people?

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )

Other:_____

INTEGRITY

How critical is the accuracy and completeness of the information?
( ) somewhat critical ( ) very critical

Are there any procedures in place to verify the accuracy of the information: ( ) No ( ) Yes

Would the corruption of this information cause:

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )

Other:_____

AVAILABILITY

How critical is the information on the system?

Public: ( ) Low ( ) Medium ( ) High ( ) Very critical
Department: ( ) Low ( ) Medium ( ) High ( ) Very critical
Branch: ( ) Low ( ) Medium ( ) High ( ) Very critical

What is the greatest length of time (in days) that the information on the system can be unavailable?
( ) 1 or less ( ) 1-2 ( ) 3-10 ( ) 11-30 ( ) 30+

Do contingencies exist to ensure recovery of the service?

Backups: ( ) Unknown ( ) No ( ) Yes
Offsite storage: ( ) Unknown ( ) No ( ) Yes
Other method of recovery:_____

Give an estimated daily cost if the allowable period of unavailability is exceeded.
Cost ($):_____

Would the destruction of this system cause:

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )

Other:_____

Signature:_____ Date:_____

Annex E – The Level-of-Granularity Numbering Scheme

Table IX (below) shows by example the methodology used in Annexes F through I to allocate components (for example, assets) into comparable levels of granularity.

Be aware that if a category cannot usefully be broken into six levels of detail, fewer levels will be needed; on the other hand, a particularly complex category might require a seventh, eighth or higher level.

Also be aware that although the numbering scheme is hierarchical, it is not necessary to "fill in missing numbers." For example, during the TRA it is acceptable to list a Level 1 category that contains only Level 6 entries. (That is, if an asset is properly a "Level 6," it should be listed as such, even if this leaves gaps in the numbering. It is important not to "promote" a minor entry to a higher level.)

Consistent use of this model to identify assets will ensure that ordinal numbers assigned during the TRA process can be combined, in a way that is mathematically valid, to yield a meaningful measurement of risk and residual risk.

Note: Different organizations might assign similar assets to different categories based on the assets' importance within each organization. If this occurs, the numbers resulting from the mathematical combination can **not** be compared between one organization and another.

Table IX – Level-of-Granularity Numbering Scheme (Examples shown: Assets)

Level 1 (Asset Category)	Level 2	Level 3	Level 4	Level 5	Level 6
Information	Personal information	Employee information	Salary	Education	High school
Process	Security processes	Crypto key management	Crypto key generation	Crypto key distribution	
Platform	Processing equipment	Workstation	Board chips	RAM	
Interfaces	Paper	Inter-organizational	Weekly		
Personnel	Contractor	Security contractor	IT security administrator	RACF specialist	
Environment	Buildings	Intrusion alarm system	Motion sensor		
Other Tangible Assets	("catch-all" category)				Batteries
Intangible Assets	Public image				

Annex F – Sample List of IT System Assets

The numbers on the assets are from a scale of granularity; full details of the numbering scheme are in Annex E. The numbers represent levels of breakdown of the asset(s) involved. The numbers do not imply any sort of ranking, but refer only to breakdown of elements. The intent of the numbers is to allow one to deal consistently with, for example, a "level 3" *information* asset with a "level 3" *physical* asset.

Many kinds of assets are listed in Annex F, as a guide to help those performing a TRA. However, not all possible assets are in this list. In any specific system, many of the assets in this list will not apply, and other assets may need to be added.

1. **INFORMATION**
   (May be stored electronically on databases or flat files, or may be paper based; also includes data during processing activities)
   2. Software *(This includes Program Source Code that is stored on/offsite; actively processing; or held by a trusted party for later retrieval by an authorized person in the event that no other copy is available [some parties think of this as escrow])*
      3. In-house *(software created within an organization by its employees or hired contractors)*
      3. Client *(software used by an organization, but which is owned by its client)*
      3. Commercial off the Shelf (COTS) *(software package purchased from a vendor)*
         4. Virus Detection Software
         4. Encryption *(software that encrypts and decrypts sensitive data)*
         4. Word Processing Software
   2. Personal *(data that would cause some level of harm to a person or organization if it were disclosed, corrupted, etc.)*
      3. Employee
         4. Salary
         4. Appraisals
         4. Medical History
         4. Bank Accounts
            5. PIN #s
               6. Account Balance
               6. Transaction Records
         4. Education
            5. Schools Attended
         4. Qualifications
         4. Service Data
         4. Criminal History
      3. Client
         4. Creditworthiness
         4. Income
         4. Liabilities
         4. Bank Accounts
            5. PIN #s

- 6. Account Balance
- 6. Transaction Records
- 4. Financial History

2. Financial
   - 3. Payroll
   - 3. General Ledger
   - 3. Accounts Payable
   - 3. Accounts Receivable
   - 3. Investment and/or Cash Flow Management Information
2. Legal
   - 3. Affidavits
   - 3. Items of Evidence
   - 3. Correspondence
   - 3. Claims
   - 3. Contracts
   - 3. Supplier / Vendor Agreements
   - 3. Attorney/Client Discussions
2. Research *(any type of scientific research that might produce a product)*
   - 3. Medical
   - 3. Aerospace *(may include defense)*
2. Planning *(data related to the running of the organization)*
   - 3. Budget
   - 3. Corporate Strategy
   - 3. Staffing Plans
2. Security *(data related specifically to the administration of security)*
   - 3. Authentication Data
     - 4. Password
     - 4. Digital Signature
   - 3. Authorization Data
     - 4. Single User
     - 4. Group
     - 4. Access Control and Labeling Tables
     - 4. Clearance Information
   - 3. Audit Logs *(Logs have uses other than security, such as system load monitoring.)*
     - 4. User Access Log
     - 4. System Activity Log
     - 4. Communication Activity Log
     - 4. Job Log
     - 4. Tape Log, etc.
   - 3. Encryption
     - 4. Digital Certificates
       - 5. Encryption Certificate
       - 5. Signature Verification Certificate
       - 5. Attribute Certificate
       - 5. Key Management Plans
       - 5. Keys

- 5. Algorithms
- 2. Maintenance Records *(historical information)*
- 2. Configuration Management Plans
  - 3. Hardware
  - 3. Source Code *(Software)*
  - 3. Communications Equipment
  - 3. Site
  - 3. Cable Plant *(all types of cabling throughout interconnecting buildings and offices)*
- 2. Documentation *(Procedural Manuals)*
  - 3. Programs *(Software)*
    - 4. Development
    - 4. Testing
    - 4. Production
  - 3. Hardware
  - 3. Systems
  - 3. Administrative
  - 3. Security Policies
    - 4. Department *(Corporate)*
    - 4. Operations
    - 4. Network
    - 4. Acceptable Use
    - 4. Onsite/Offsite Media Storage
    - 4. Contingency Plan
    - 4. Disaster Recovery Plan *(Business Resumption Plan)*
  - 3. Configuration
    - 4. Hardware
    - 4. Source Code *(Software)*
    - 4. Communications Equipment
    - 4. Cabling and Protocol Information
    - 4. Site
- 2. Onsite and Offsite Backups *(Archived Data)*
  - 3. Configuration Information *(file system structures, .ini files, etc.)*
  - 3. Operating System Data
  - 3. Source Code Data
  - 3. Application Data
- 2. Electronic Mail *(E-mail*)
  - 3. Messages
  - 3. Attachments
    - 4. Documents
    - 4. Executable Programs
    - 4. Graphics
    - 4. Audio and Video Files
    - 4. Macros
- 2. Voice Mail *(V-mail)*
  - 3. Messages
  - 3. Tape Backup

2. Facsimile (Electronic and Paper)
2. Data Specific to National Interest
    3. Cabinet (and Ministry level)
    3. Armed Forces
        4. Defense Plans
            5. Defense Contingency Plans
            5. Deployment Data
            5. Inventories
        4. Tactical Assets
            5. Platforms *(tanks, ships, helicopters, etc.)*
            5. Shelters
2. Data Specific to International Interest *(other allied sources, agencies and nations)*
    3. Cabinet *(and Ministry level)*
    3. NATO
    3. Information from Allied Sources, Agencies and Nations
    3. Embassy Documents
    3. Armed Forces
        4. Defense Plans
            5. Defense Contingency Plans
            5. Deployment Data
            5. Inventories
        4. Tactical Assets
            5. Platforms *(tanks, ships, helicopters, etc.)*
            5. Shelters

1. <u>PROCESSES</u>

(The fundamental steps in creating, processing, transmitting, maintaining and reporting of the information assets) Processes can be performed by paper-based or mechanical methods as well as electronically. Sensitivities of process assets do not refer to the underlying data but rather to the activities used to manipulate or process those data.

2. Operating System Programs
    3. Single User O/S
        4. User Interface
        4. I/O
        4. Control
        4. Communications
        4. Management
        4. Multi-tasking
    3. Multi-User O/S
        4. User Interface
        4. I/O
        4. Control
        4. Communications
        4. Management
        4. Multi-tasking
        4. Virtual Machine

2. Application Programs
    3. Single User
    3. Shared
2. Communication Programs
2. Management and Administration Programs
    3. Utility Programs
    3. Diagnostic Programs
    3. Network Monitoring Programs
2. User Application Programs *(screens for data entry)*
2. User
    3. Data Manipulation
    3. Control
    3. Communications
    3. Scientific
2. Management
    3. Personnel
    3. Financial
    3. System
    3. Approval
    3. Inventory
    3. Configuration Control
2. Telework
    3. Data Manipulation
    3. Requesting Processes
        4. Application Updates
        4. Reports
    3. Uploading and/or Downloading Data
    3. Security Related Processes
        4. Virus Checking
        4. Identification & Authentication
2. Planning *(related to internal decision-making processes of an organization)*
2. Reporting
    3. Security Incident Reports
        4. Investigation
        4. Historical, e.g., virus infections
    3. IT Equipment Outage Reports
2. Security
    3. Creation and maintenance of User Profiles
    3. Creation and maintenance of Group Profiles
    3. Cryptographic Key Management
        4. Key Generation
        4. Key Use
        4. Key Disposal
    3. Certificate Management
        4. Certificate Generation
        4. Certificate Use

4. Certificate Disposal

1. PLATFORMS

2. Processing Equipment
    3. Workstations
        4. CPU Chips
        4. Drives
            5. Hard Disk *(removable and attached)*
            5. Floppy Disk
                6. Diskettes *(includes new diskettes)*
            5. Tape
                6. Tapes *(includes new tapes)*
            5. CD-ROM
                6. CDs *(includes new CD Blanks)*
            5. Read/Write CD
            5. WORM CD *(Write Once Read Many CD)*
            5. Zip Drives
        4. Network Interfaces
        4. Boards
            5. Memory
                6. RAM
                6. ROM
                6. Cache
                6. VRAM
        4. Monitors
        4. Keyboards
        4. Printers
            5. Laser
                6. Printer Paper
                6. Forms
                6. Ink
                6. Toner
            5. Impact *(Pin)*
                6. Printer Paper
                6. Forms
                6. Ribbons
        4. Multimedia Components
            5. Flatbed Scanners
            5. Audio Speakers
            5. Video Cameras
            5. Microphones
            5. Microfilm/Fiche Output
    3. Laptops and Notebooks
        4. PCMCIA Cards
        4. Portable Modems
        4. Removable Disk Drives

3. LAN Servers
    4. CPU Chips
    4. Drives
        5. Hard disk *(removable and attached)*
        5. Floppy disk
            6. Diskettes *(includes new diskettes)*
        5. Tape
            6. Tapes *(includes new tapes)*
        5. CD-ROM
            6. CDs *(includes new CD Blanks)*
        5. Read/Write CD
        5. WORM CD *(Write Once Read Many CD)*
    4. Disk Cartridges
    4. Network Interfaces
    4. Boards
        5. Memory
            6. RAM
            6. ROM
            6. Cache
            6. VRAM
    4. Monitors
    4. Keyboards
    4. Printers
        5. Laser
            6. Printer Paper
            6. Forms
            6. Ink
            6. Toner
        5. Impact *(Pin)*
            6. Printer Paper
            6. Forms
            6. Ribbons
    4. Multimedia Components
        5. Flatbed Scanners
        5. Audio Speakers
        5. Video Cameras
        5. Microphones
        5. Microfilm/Fiche Output
3. Minis
    4. CPU
    4. Drives
        5. Disk
            6. Disks *(also removable type; includes new disks)*
        5. Tape
            6. Tapes *(includes new tapes)*
        5. CD

- 6. CDs *(includes new CD Blanks)*
- 5. Read/Write CD
  - 6. CDs *(includes new CD Blanks)*
- 5. WORM CD *(Write Once Read Many CD)*
  - 6. CDs *(includes new CD Blanks*)
- 4. Network Interfaces
- 4. Boards
  - 5. Memory
    - 6. RAM
    - 6. ROM
    - 6. Cache
    - 6. VRAM
- 4. Monitors
- 4. Keyboards
- 4. Printers
  - 5. Printer Paper
  - 5. Forms
  - 5. Ribbons
  - 5. Ink
  - 5. Toner

3. Mainframes
   - 4. CPU
   - 4. Drives
     - 5. Disk
       - 6. Disks *(includes new disks)*
     - 5. Tape
       - 6. Tapes *(includes new tapes)*
   - 4. Network Interfaces
   - 4. Boards
     - 5. Memory
       - 6. RAM
       - 6. ROM
       - 6. Cache
       - 6. VRAM
   - 4. Monitors
   - 4. Keyboards
   - 4. Printers
     - 5. Printer Paper
     - 5. Forms
     - 5. Ribbons
     - 5. Ink
     - 5. Toner
3. Facsimile Machines
   - 4. Fax Paper

2. Communications (Network) Components
   3. Routers

    4. Cables
3. Modems
    4. Cables
3. Bridges
    4. Cables
3. Telephones
    4. STU III *(crypto)*
        5. Cables
    4. Cellular

1. <u>INTERFACES</u>

(Includes manual and electronic transfer of data: those elements that provide the capability to communicate between major system components or through the system boundary.)

2. Network Connections
2. Disk and Tape
2. Paper

1. <u>PERSONNEL</u>

(Employees and Contractors who have some level of authorized logical access to IT systems, and/or physical access to the site.)

2. Employees
    3. Corporate Managers
    3. Operations Managers
    3. Operations Staff
    3. Software Developers
    3. Software Maintenance
    3. Client/Server Technicians
    3. Hardware Maintenance Technicians *(Mainframe & Mini)*
    3. LAN and/or WAN Administrators
    3. Users
        4. Data Entry *(also those who manipulate data and produce reports)*
    3. Security
        4. IT Security Officers
        4. IT Security Administrators
        4. Physical Security Guards
    3. Couriers
    3. Lawyers
    3. Auditors
    3. Accountants
2. Maintenance *(of the Physical Environment)*
    3. Electricians
    3. Plumbers
    3. Air Conditioning maintainers
    3. Cleaning staff *(Housekeeping Staff)*
    3. Technicians for Fire Extinguishing Systems

2. Contractors
    3. Operations Managers
    3. Operations Staff
    3. Software Developers
    3. Software Maintenance
    3. Client/Server Technicians
    3. Hardware Maintenance Technicians *(Mainframe & Mini)*
    3. LAN and/or WAN Administrators
    3. Users
        4. Data Entry *(also those who manipulate data and produce reports*)
    3. Security
        4. IT Security Officers
        4. IT Security Administrators
        4. Physical Security Guards
    3. Couriers
    3. Lawyers
    3. Auditors
    3. Accountants
    3. General Business
2. Maintenance *(of the Physical Environment)*
    3. Electricians
    3. Plumbers
    3. Air Conditioning maintainers
    3. Cleaning staff *(Housekeeping Staff)*
    3. Technicians for Fire Extinguishing Systems

1. <u>ENVIRONMENT</u>

(The physical aspect of the site and the environmental controls)

2. Building(s)
    3. Access Lanes
    3. Intrusion Alarm Systems
        4. Monitoring Controls for Area Surveillance
        4. Motion Sensors
2. Data Centre(s)
2. Server Room(s)
2. Technical Infrastructure Room(s) *(Wiring Closets)*
2. Media Storage Room *(Archives)*
    3. Cabinets
    3. Tape Racks
    3. Safes
2. Environmental Controls
    3. Fire Suppression
    3. Fire Fighting
    3. Fire Alarms
    3. Uninterruptable Power Supply
    3. Power Conditioning *(filtering)*

3. Air Conditioning
3. Water Supply *(plumbing)*
3. Electrical Power
3. Heating
3. Lighting

2. Office
3. Business
3. Home *(Teleworkers)*
3. Hotels, Motels, etc. *(frequently used by Mobile Teleworkers)*

1. <u>OTHER TANGIBLE ASSETS</u>

(Assets that do not fit well elsewhere and may need a new category or sub-category created for them)

1. <u>INTANGIBLE ASSETS</u>

(Non-physical assets that are difficult to value, but which have a major effect on the organization)

2. Goodwill
2. Service to Clients
2. Public Confidence
2. Public Trust
2. Competitive Advantage
2. Morale
2. Ethics
2. Productivity
2. Loyalty

Annex G – Sample List of Threat Agents

The numbers on the threat agents are from a scale of granularity; full details of the numbering scheme are in Annex E. The numbers represent levels of breakdown of the threat agent(s) involved. The numbers do not imply any sort of ranking, but refer only to breakdown of elements.

Threat Agents can cause harm/injury to an organization and its assets. They include:

1. **NON-HUMAN**
    2. Random
        3. IT Malfunctions
            4. Software Bugs
            4. Computer Component Failure
            4. Network Failure
            4. Hardware Failure
        3. Nature *(acts of God)*
            4. Earthquake
            4. Flood
                5. Rivers
                5. Dikes
                5. Dams
                5. Rain
            4. Lightning Strikes
                5. Power Surge
                5. Fire
            4. Wind
                5. Tornadoes
                5. Hurricanes
        3. Physical Environment
            4. Electrical
                5. Fire
                5. Blackouts
                5. Brownouts
                5. Unannounced Power Failure *(electrical maintenance)*
                5. Localized Power Failure *(single floor; e.g., electrical maintenance)*
            4. Spontaneous Combustion
                5. Fire
            4. Water
                5. Sprinklers
                5. Washrooms *(Water Closets)*
                5. Damaged Plumbing *(accidental breakage or freezing)*
                5. Condensation
            4. Air
                5. Dust
                5. Noxious Fumes
    2. Non-random *(initiated by humans)*

3. Malicious Code
    4. Trojan Horses
    4. Viruses
    4. Macro Viruses
    4. Application Programs *(errors in source code)*
3. Explosive devices
    4. Bombs
    4. Land Mines
3. Jammers *(jamming of communication lines)*
3. Arson
    4. Fire
3. False Alarms
    4. Fire

1. <u>HUMAN</u>

2. Internal *(Employees and Contractors who have some level of authorized logical access to IT systems, and/or physical access to the site)*
    3. Management
        4. Corporate Managers
        4. Operations Managers
    3. Technical Staff
        4. Computer Operators
        4. Systems Analysts
        4. Software Developers
        4. Software Maintenance
        4. Client/Server Technicians
        4. Hardware Maintenance Technicians *(Mainframe & Mini)*
        4. LAN and/or WAN Administrators
    3. Non-technical Staff *(Users who have authorized access to the site, and/or who have authorized physical/logical access to data)*
        4. Receptionist
        4. Payroll Staff
        4. Finance Staff
        4. Accounting Staff
    3. Security
        4. IT Security Officers
        4. IT Security Administrators
        4. Physical Security Guards
    3. Courier Services
        4. Couriers
    3. Business Professionals
        4. Lawyers
        4. Auditors
        4. Accountants
    3. Environmental Controls
        4. Electricians

    4. Plumbers
    4. Air Conditioning Technicians
    4. Fire Suppression Systems Technicians
3. Building Maintenance
    4. Cleaning staff *(Housekeeping Staff)*
    4. Electricians
    4. Plumbers
    4. Air Conditioning maintainers
    4. Carpenters
    4. Masons
    4. Telephone maintainers

2. External *(People who have no authorized logical access to IT systems, and/or no authorized physical access to the site)*
    3. Foreign Government Intelligence Agents
    3. Industrial/Commercial Intelligence Agents *(Corporate Raiders)*
    3. Hackers
        4. Browsers
    3. Criminal elements and organizations
    3. Terrorists *(religious, political, etc.)*
    3. News Media
        4. Reporters
            5. Television
            5. Print
        4. Photographers
            5. Television
            5. Print

Annex H – Sample List of Threat Events

The numbers on the threat events are from a scale of granularity; full details of the numbering scheme are in Annex E. The numbers represent levels of breakdown of the threat event(s) involved. The numbers do not imply any sort of ranking, but refer only to breakdown of elements.

1. ESPIONAGE
- 2. Foreign Intelligence
- 2. Industrial/Commercial Intelligence
- 2. News Media
- 2. Hackers

1. SABOTAGE
- 2. Foreign Intelligence
- 2. Industrial/Commercial Intelligence
- 2. Criminal Activity
- 2. Labour Unrest
- 2. Staff Termination (*Unfriendly*)
- 2. External Activists
- 2. Denial of Service

1. SUBVERSION
- 2. Foreign Intelligence
- 2. Industrial/Commercial Intelligence
- 2. Criminal Activity
- 2. Lobbyist Activities
- 2. Propaganda Activities
- 2. Misuse/Abuse of Equipment
- 2. Impersonation
- 2. Tampering
- 2. Information Overload
- 2. Denial of Service

1. TERRORISM
- 2. Criminal Activity
- 2. Loss of Personnel
- 2. Tampering
- 2. Terrorist Activities
- 2. Riots
- 2. Denial of Service

1. CRIMINAL ACTS
- 2. Criminal Activity

2. Forcible Entry
2. Blackmail
2. Verbal/Physical Attacks
2. Misuse/Abuse of Equipment
2. Staff Termination (*Unfriendly*)
2. Impersonation
2. Tampering
2. Piracy
2. Denial of Service

1. ACCIDENTS

2. Loss or shortage of Personnel
2. IT Malfunctions
2. Cryptographic Failure
2. Power Failure
2. Water Failure
2. Failure of Environmental Controls
2. Non-delivery/Missed Delivery of IT Related Data
2. Static Discharge
2. Emergency Evacuation
2. Denial of Service

1. FRAUD

2. Embezzlement
2. Forgery
2. Theft of Data
2. Theft of Equipment
2. Theft of Services
2. Manipulation of Data

1. INTERCEPTION

2. Criminal Activity
2. Foreign Intelligence
2. Industrial/Commercial Intelligence

1. PENETRATION

2. Criminal Activity
2. Foreign Intelligence
2. Industrial/Commercial Intelligence

1. NATURAL HAZARDS

2. Geological Activity
2. Weather

2. Disease
2. Animal Infestation

1. INSURRECTION

2. Terrorist Activities
2. Foreign Intelligence

1. MISREPRESENTATION

2. Criminal Activity
2. Foreign Intelligence
2. Industrial/Commercial Intelligence

Annex I – Sample List of Vulnerabilities

The numbers on the vulnerabilities are from a scale of granularity; full details of the numbering scheme are in Annex E. The numbers represent levels of breakdown of the vulnerabilities involved. The numbers do not imply any sort of ranking, but refer only to breakdown of elements.

1. EXTERNAL

- 2. Technical
  - 3. Identification, Authentication and Authorization
    - 4. Inadequate IA&A of sender and receiver
    - 4. Insufficient proof of sending or receiving of messages, transactions, etc.
    - 4. Transfer of passwords or keys in the clear
    - 4. Lack of or inadequate access control management
    - 4. Lack of or inadequate access change control
    - 4. Lack of or insufficient audit trail
    - 4. Infrequent changing of passwords
    - 4. Use of weak passwords
  - 3. Physical Access
    - 4. Lack of or inadequate monitoring of physical traffic flow
    - 4. Lack of or inadequate monitoring of laneways
    - 4. Inadequate audit trail of video monitors
    - 4. Inadequate monitoring of elevators and staircases
    - 4. Inadequate access control mechanisms for elevators and staircases
    - 4. Unstable power grid
  - 3. Network Access
    - 4. Inadequate logical access controls
    - 4. Inadequate protection of data communications
    - 4. Inadequate protection of communications media
    - 4. Lack of or insufficient audit trail
    - 4. Excessive complexity of the system
    - 4. Complicated user interface
    - 4. Network not powered down during fire drill
- 2. Procedural
  - 3. Identification, Authentication and Authorization
    - 4. Insufficient monitoring of IT security procedures
    - 4. Inadequate authorization changes for new, transferred or terminated personnel
    - 4. Lack of or inadequate formal notification procedures between human resources and technical services about UserID creation and deletion for new, transferred or terminated personnel
    - 4. Inadequate dial-in/out procedures and compliance
    - 4. No dial-in/out auditing performed
  - 3. Documentation
    - 4. Lack of or insufficient security policies
    - 4. Lack of or insufficient contingency plan
    - 4. Lack of or insufficient disaster recovery plan (business resumption plan)

4. Lack of or inadequate emergency measures procedures
4. No clear crisis management policies and documented procedures in place

3. Physical Access
4. Lack of or insufficient security policies
4. Lack of or insufficient audit trail

1. <u>SYSTEM</u>

2. Technical
3. Identification, Authentication and Authorization
4. Lack of or inadequate access control management
4. Lack of or inadequate access change control
4. Lack of or insufficient audit trail
4. Infrequent changing of passwords
4. Use of weak passwords

3. Physical Access
4. Lack of or inadequate monitoring of physical traffic flow
4. Lack of or insufficient audit trail

3. Network Access
4. Inadequate logical access controls
4. Inadequate protection of data communications
4. Inadequate protection of communications media
4. Lack of or insufficient audit trail
4. Lack of or inconsistent review of audit logs
4. Excessive complexity of the system
4. Complicated user interface
4. Network not powered down during fire drill
4. Connection of computers handling different security levels

2. Procedural
3. Identification, Authentication and Authorization
4. Infrequent changing of passwords
4. Use of weak passwords
4. Inadequate authorization changes for new, transferred or terminated personnel
4. Lack of or inadequate formal notification procedures between human resources and technical services about UserID creation and deletion for new, transferred or terminated personnel

3. Physical Access
4. Network not powered down during fire drill
4. Unsupervised work of cleaning or outside staff
4. Unmonitored physical traffic flow
4. Lack of or insufficient audit trail
4. Lack of or insufficient review of audit logs
4. Improper location of room
4. Access list not located at restricted access rooms
4. No true floor to ceiling walls around restricted access rooms

1. <u>OBJECT</u>

2. Technical

3. Identification, Authentication and Authorization
    4. Lack of or insufficient program checks to detect unauthorized modification
    4. Inadequate verification of incoming data
3. Physical Access
    4. Connection of computers handling different security levels
    4. Uncontrolled viewing of data
3. Network Access
    4. Inconsistent logout compliance
    4. Complicated user interface
    4. Excessive complexity of the system
    4. Uncontrolled copying of data
    4. Uncontrolled re-use of data

2. Procedural
    3. Misuse of call forwarding
    3. Misuse of computer resources
    3. Personnel allowed access to sensitive data before clearances completed
    3. Inconsistent hiring and screening procedures for new and contract personnel
    3. Lack of readily accessible base documents (*paper or electronic*)
    3. Lack of or insufficient audit trail
    3. Lack of or inconsistent review of audit logs
    3. Inadequate inventory of software (*configuration management*)
    3. Inadequate storage of original software disks and CDs
    3. Uncontrolled importing of software
    3. Application design limitations
    3. Faulty compilers and debuggers
    3. Uncontrolled manipulation of coding
    3. Incorrect application of the technology (*System Conceptualization*)
    3. Erroneous, incomplete, or inconsistent requirements definition
    3. Flaws in design or specifications
    3. Analysis of system concepts and design based on false assumptions
    3. Poor selection of programming language
    3. Misleading development tools
    3. Inadequate synchronization and implementation of software releases (*configuration management control*)
    3. Incompatible versions of software
    3. Inadequate quality control procedures
    3. No separation of development and production environments
    3. No recovery process for legacy systems
    3. Data conversion problems
    3. Incomplete testing and evaluation of source code
    3. Erroneous verification of source code
    3. Inadequate verification of incoming data
    3. Mistakes in debugging of source code
    3. Not acting upon known flaws in source code
    3. Faulty maintenance after installation of software
    3. Faulty upgrades of software

3. Date related errors (*leap year, century, "Y2K"*)
3. Introduction of new flaws in source code in attempts to fix old flaws
3. Premature removal of backups
3. Premature archival or destruction of supporting documents
3. Inadequate decommissioning procedures for applications
3. Lack of or insufficient backups
3. Lack of or inadequate separation of responsibilities for administration personnel
3. Uncontrolled copying of data
3. Uncontrolled re-use of data
3. Uncontrolled viewing of data
3. Uncontrolled use of recovery utilities
3. Inadequate access control administration procedures
3. Erroneous parameter settings for programs
3. Use of default parameter settings for security software
3. Lack of readily accessible base documents (*paper and electronic*)
3. Lack of or insufficient program checks to detect errors
3. Lack of or insufficient change control management
3. Lack of or insufficient number of copies of procedural manuals
3. Inadequate security incident reporting procedures
3. Inadequate disposal of manuals with sensitive information
3. Incorrect labeling of contents/sensitivity level for storage media
3. Inadequate protection of storage media against destruction, damage or loss during delivery to recipient
3. Inadequate protection of storage media against destruction, damage or loss while in storage
3. Distribution of storage media to wrong recipient
3. Inadequate sanitation of storage media before recycling or disposal
3. Distribution of E-mail to wrong recipient
3. Lack of or inadequate E-mail acceptable use agreement
3. Lack of or inadequate procedures for E-mail use
3. Distribution of voice mail to wrong recipient
3. Lack of or inadequate procedures for voice mail use
3. Inadequate storage of fax paper with sensitive information
3. Insufficient routine virus monitoring
3. Infrequent update of virus detection software
3. Desktop or portable workstations (*laptops, notebooks*) not sanitized before repair or disposal
3. Lack of or inadequate maintenance of environmental controls
3. Lack of or inadequate monitoring of environmental controls
3. Installation of equipment and components by unskilled personnel
3. Workstations not configured according to Technical Services Baselines
3. Communications equipment not configured according to Technical Services Baselines
3. No Uninterruptable Power Supply for servers

1. <u>PERSONNEL</u>

2. Accessibility (*Availability*)

    3. Lack of or insufficient personnel
    3. Lack of or insufficient backup or shadowing for key personnel
2. Knowledge
    3. Poor adjustment to technological changes
    3. Editing mistakes
    3. Mistakes in debugging of source code
    3. Incorrect keying of data
    3. Lack of or insufficient knowledge of configuration management plans by responsible personnel
    3. Lack of or insufficient knowledge of security policies
2. Training
    3. Inconsistent logout compliance
    3. Lack of security orientation and awareness for personnel
    3. Lack of or insufficient training of personnel in use of processing equipment
    3. Lack of or insufficient training of personnel in use of fire extinguishing equipment
    3. Lack of or insufficient training of personnel for job related activities
    3. Lack of or insufficient training of personnel for dealing with verbal/physical attacks
    3. Lack of or insufficient training of personnel for dealing with threats by telephone, fax or E-mail
    3. Lack of or insufficient training of personnel on use of environmental controls
2. Procedural
    3. Poor employer - employee relationship
    3. Lack of visible security commitment by management
    3. Lack of or insufficient separation of personnel responsibilities
    3. Inconsistent hiring and screening procedures for new and contract personnel

Annex J – Threats to Assets through Vulnerability Interrelationships

Threat Agent(s)	Motivation	Capability	Threat	Vulnerability	Asset	Consequences	Safeguard(s)
Hackers	-Challenge -Status	-Knowledge	-Unauthorized Access	-Configuration	-Business data -Privileges	-Disclosure -Modification -Embarrassment	-Technical -Administrative -Personnel -Security awareness
Foreign Intelligence	-Political gain -Economic advantage	-Skills	-Unauthorized Access -Unauthorized Use	-Configuration -Physical Access -Employees	-Business data	-Disclosure	-Technical -Physical -Personnel -Awareness
Criminal Activity	-Financial gain	-Skills	-Service Denial -Theft	-Configuration -Physical Access	-Business data	-Disclosure -Modification -Destruction	-Technical -Physical -Personnel -Awareness
Corporate Raiders	-Financial gain -Economic advantage	-Skills -Resources	-Takeover -Hire away	-Salaries -Working conditions	-Employees -Knowledge	-Loss of talent	- Salaries -Working conditions
Vandals & Terrorists	-Revenge	-Disgruntled Employee -Outside personnel -Labour Problems	-Damage -Service Denial -Theft	-Configuration -Physical Access -Salaries -Working Conditions	-Employees -Facility	-Destruction -Modification -Productivity -Service Denial -Looting	-Technical -Physical -Personnel -Awareness
Employees (insiders)	-Human error		-Damage -Service Denial -Destruction -Modification	-Configuration -Fatigue -Training -Knowledge	-Business data -Application programs	-Destruction -Modification -Productivity -Service Denial -Embarrassment	-Technical -Physical -Personnel -Awareness
Electrical Storm		-Varying degrees of severity	-Damage -Service Denial -Destruction -Safety		-Building -IT Systems	-Destruction -Modification -Productivity	-Alternative supply -Redundancy -Business resumption Plan

The table above serves only as an example of the type of threat agents and how they inter-relate among some kinds attacks in terms of threats, vulnerabilities of some assets and consequences. Note that a Threat Agent may act through more than vulnerability resulting in more than a single consequence.

ANNEX K – GLOSSARY

Acceptable Level of Risk	A judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that an information technology (IT) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of IT assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements. (Based on OPNAVINST 5239.1A)
Access	A specific type of interaction between a subject or entity and an object or resource which results in a flow of information from one to another or in the subject or entity changing the observable properties of the object or resource. For example, the logging on to a computer system for the purpose of gaining entry to a word processing application or gaining entry to stored information. (New)
Access Control	A method of controlling access to IT resources so that only an authorized entity or entities may access authorized resource(s) by authorized means.(New)
Access Control List	A list of subjects, users or entities, together with their access rights, which are authorized to have access to a resource. (Based on ISO 7498-2)
Access Control Mechanism(s)	Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an IT resource system. (Based on DOE 5636.2A)
Access Mode	A distinct operation recognized by the protection mechanisms as a possible operation on an object. Read, write and append are possible modes of access to a file, while execute is an additional mode of access to a program. (MTR-8201)
Access Permission; Access Right	Permission for a subject or entity to access a particular object or IT resource in a specific access mode, (e.g.: to read a file but not write to it). (Based on ISO 2382-08)
Access to Information	The function of providing to members of the public, upon their

	request, the government information to which they are entitled under law. (A-130)
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity. (Based on ISO 7498-2)
Accreditation	Formal declaration by the responsible management authority approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. (MG03; TSEG)
Administrative Security	The management constraints; operational, administrative, and accountability procedures and supplemental controls established to provide an acceptable level of protection for information and assets. (OPNAVINST 5239.1A; FIPS PUB 39; DOE 5636.2A)
Aggregation	Individual items of information can each be assigned a sensitivity level. However, the sensitivity of a collection of information, considered as a whole, may be greater that the sensitivity of any of the individual parts. This sensitivity of the information in aggregate is an important consideration in determining the overall security required for an IT system or a collection of systems. (CID/09/17)
Annual Loss Expectancy (ALE)	The ALE of an IT system or activity is the expected yearly dollar value loss from the system or activity by attacks against its assets. (Based on OPNAVINST 5239.1A)
Application Software	Routines and programs designed by, or for system (functional) users and customers. (Adapted from AFR 205-16)
Approval-in-principle	For certain documentation, such as the security architecture, project or system managers may require an approval-in-principle from security authorities in order to proceed toward implementation. An approval-in-principle signifies that the proposed concept is acceptable. It is not, however, an authority to process. (GSP)
Architecture	A description of a system and its structure. In each structural component, the various elements or entities, their properties and their inter-relationships are explicitly defined. (CIS/01/6/2)
Asset	A component or part of the total system or network to which the department directly assigns a value to represent the level of

	importance to the "business" or operations/operational mission of the department, and therefore warrants an appropriate level of protection. Assets types include: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image. (Based on MG03).
Asset Value	A measure of asset worth in terms of replacement cost, confidentiality, integrity and availability. (FASO TRA SIG)
Assurance	The degree of confidence that the implemented security functions of an IT system or product adequately enforce the system security policy. Alternatively, the degree of confidence that the implemented system meets its stated security requirements. (CIS/01/6/2)
Asymmetric Cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that given the public transformation it is computationally infeasible to derive the private transformation. (ISO/IEC 11770-1)
Attack	The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place. (Based on NCSC)
Audit	The process of conducting an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures. (CAG) *See Security Audit*
Audit Trail	A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports and/or backward from records and reports to their component source transaction. (CSC-STD-001-83)
Authentication	The act of verifying the claimed identity of an entity. (NSAI)
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed and applies to entities such as users, processes, systems and information. (ISO 7498-2)

Authorization	The granting of rights, which includes the granting of access based on access rights. (ISO 7498-2)
Availability	The accessibility of systems, programs, services and information to authorized users when needed and without undue delay. (MG01)
Average Loss Expectancy (ALE);	*See Annual Loss Expectancy*
Backdoor	*See Trap Door*
Backup	Provision and procedures for continued operation of a system and for recovery of the data files, program libraries, and replacement data processing systems and facilities after a disaster, system failure, or any type of damage. (CAG)
Backup Plan	*See Contingency Plans*
Baseline	An element of a system which cannot be changed without formal approval. (MG02)
Baseline Controls	A minimum set of safeguards established for a system or organization. (ISO 7498-2)
Basic Reliability Check	An assessment to determine the trustworthiness of individuals; condition for being granted basic reliability status. (GSP)
Basic Reliability Status	The minimum type of personnel screening; allows access to non-sensitive information and assets only. (GSP)
Bastion Host	A term that is used to describe a firewall that is configured to act as an external guard to a network. (New)
Biometric	Pertaining to the use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of individuals. (ISO 2382-8)
Black	A term that applies to IT systems and communications media that process or handle unclassified information or that the confidentiality of the information is protected by approved cryptography. (NEW)

Breach of Security	When any sensitive information and/or assets have been compromised. Without restricting its scope, a breach may include compromise in circumstances that make it probable that a breach has occurred. (GSP)
Business Resumption Planning	The process of developing a plan to restore business operations in the event of an interruption. (GSP)
Certification	The comprehensive assessment of the technical and non-technical security features of an information system/network and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular design and implementation meets a specific set of security requirements. Certification evidence provided must satisfy accreditation requirements and all certification activities must be completed before the accreditation can be finalized. (CAG)
Certification and Accreditation Plan	In order to ensure that all documentation and other security requirements are addressed, this plan is developed by system security/management staff or project staff. By way of introduction, a brief system description is provided. The plan identifies what activities are required to get a system certified and accredited, which organization is responsible for each activity, and any time frames which must be met. (CAG)
Checksum	A value calculated from a block of data and used to detect unauthorized modification and/or errors in stored and transmitted data. (Based on MG01)
Classification	A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. (Based on CSC-STD-004-85)
Classified Assets	Assets, other than information, that are important to the national interest and therefore warrant safeguarding. (GSP)
Classified Information	Information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and the compromise of which would reasonably be expected to cause injury to the national interest. (GSP)

Cold Site	An alternate processing facility with essentials in place such as environmental controls and cabling, but with no computing equipment, furnishings or staff. (New)
Collusion	The act of two, or more, agents or perpetrators cooperating or conspiring to perpetrate an intentional event. (Based on NCSC-WA-001-85)
Communications Security (COMSEC)	Protection resulting from applying cryptographic, transmission and emission security measures to telecommunication emissions, and information handling equipment, and from applying other measures appropriate to COMSEC information and material. COMSEC also includes the instruction required to effect this protection. These measures are designed to prevent compromise of information stored, transmitted or processed on an IT system. COMSEC is also designed to ensure the authenticity of telecommunications. (New)
Compromise	A violation of the security policy of a system or network such that an unauthorized disclosure, modification, removal, interruption or destruction of sensitive information may have occurred. (Based on NCSC-WA-001-85)
Computer	A machine capable of accepting, performing calculations on or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices. (DODD 5200.28)
Computer Fraud	Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or coverup of the act, or series of acts through improper manipulation of: (a) input data; (b) output or results; (c) applications programs; (d) data files; (e) computer operations; (f) communications; or (g) computer hardware, systems software, or firmware. (CSA Vocab.)
Computer Security (COMPUSEC)	The protection resulting from measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, destruction, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system. (CAG)
Computer Security Incident	An adverse event associated with an IT system(s): (a) that is a failure to comply with Departmental security regulations or directives; (b) that results in suspected or actual compromise of

	classified information; or (c) government property or information. (Adapted from DOE 5636.2A)
Confidential	The level of classification that applies to information and assets when compromise could reasonably be expected to cause injury to the national interest; in capital letters, a mark to indicate level of sensitivity. (GSP)
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 7498-2)
Concept of Operations	This document provides basic information regarding the operation of the system and often forms the basis for security recommendations. The Concept of Operations must include, at a minimum: a description of the system, including any external connections; data sensitivity information and access limitations; the user communities for specific applications and equipment; personnel or positions responsible for operations, administration, and maintenance; and anticipated modification/expansion of the system. The Security Concept of Operations must include: the security organization, including personnel and proposed duties and responsibilities. (CAG)
Configuration	The arrangement of a computer system or network as defined by the nature, number, the interconnection, and chief characteristics of its functional units. This term may refer to a hardware configuration or a software configuration. (CAG)
Configuration Management	The management of changes made to a system's hardware, software, and firmware and to the documentation which chronicles changes to the equipment, personnel and security systems throughout the development and operational life of the system. (CAG)
Configuration Management Plan	A plan used to identify how hardware and/or software changes will be conducted on the system. It also defines the roles and responsibilities of the organization involved in configuration management of the system.(CAG)
Consequence	The result of the occurrence of a threat event, expressed as a (usually undesirable) change in the state of security for an asset or information. (MBW2) *Synonymous with Impact and Injury*
Contingency	Any unexpected event affecting the availability of an IT system (e.g.: a disaster requiring facility relocation; failure requiring

	on-site recovery; and any event causing personnel evacuation). (Other)
Contingency Management	Management of all the actions to be taken before, during, and after an emergency condition, along with documented, tested procedures which, if followed, will ensure the availability of critical IT systems and which will facilitate maintaining the continuity of operations in an emergency situation. It consists of all preparations required to recover from short interruptions of service to a full disaster situation. The term Adisaster@ should be taken to mean any condition that may cause an IT system or network to fail to provide the necessary service. For example, a virus which infects an IT system or network and perhaps deletes files may be considered a Adisaster.@ (Adapted from DOE 5636.2A) This term needs to be expanded to include contingency planning which may fall outside the scope of Adisasters@. For example, damage control planning for, and the containment of, virus attacks.
Contingency Plan	A plan for emergency response, backup operations, and post-disaster recovery maintained by an IT activity as part of its security program. A comprehensive consistent statement of all the actions (plans) to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical IT resources and which will facilitate maintaining the continuity of operations in an emergency situation. (Based on OPNAVINST 5239.1A; NCSC-WA-001-85)
Contingency Planning	The process of developing a plan to restore information technology operations in the event of a disruption. (GSP)
Continuity of Operations	The maintenance of essential services for an information system after a major failure. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage). (GAO)
Controlled Access	Either part or all of an environment where all types and aspects of an access are checked and controlled. (AFR 205-16) *Synonymous with Controlled Access Area*
Controlled Accessibility	Synonymous with Access Control
Controlled Area	An area comprised of any combination of the three restricted zones. (GSP)

Controlled Cryptographic Item (CCI)	Secure telecommunications or information handling equipment, or associated cryptographic component or ancillary device that is unclassified when unkeyed (or when keyed with an unclassified key) but controlled through an accounting system. (GSP)
Correctness	The degree of confidence that exists in the consistency between a specification and its implementation. It may be between requirements and technical specification or between technical specification and physical or logical implementation. (Adapted from MTR-8201) *See also Verification*
Cost Benefit Analysis (CBA)	An assessment in terms of cost of the protection to be gained by implementing appropriate safeguards versus the cost or harm that would occur due to loss, modification, destruction or compromise of information without the implementation of appropriate safeguards. (New) *Synonymous with Cost-Risk Analysis*
Countermeasure	Any action, device, procedure, technique, or other measure that may be used in one or more of the three protective areas: detection, prevention and recovery to reduce the vulnerability of an IT system or activity to the realization of a threat. To be effective the countermeasure should be complete, correct, and self-protecting. Also called a mechanism. (New)
Covert Channel	A channel, not normally intended for communications, that allows a process to transfer information in a manner that violates the system security policy. (CAG)
Cracker	All persons, criminal or otherwise, who penetrate or attempt to penetrate computer or communication networks without authorization. (New)
Criticality	A concept related to the mission the automated system supports and the degree that the mission is dependent upon the system. This degree of dependence corresponds to the effect on the mission in the event of denial of service, modification, or destruction of data or software. (AFR 205-16)
Cryptanalysis	A process used to analyse encrypted information for the purpose of deriving the original cleartext and/or the key used to encrypt that information. (NEW)Cryptographic Security
(CRYPTOSEC)	The protection provided to an IT system(s) or network(s) by the proper use of technically sound crypto-systems or components to

	provide assurance in confidentiality and integrity. (Adapted from AMSG 524)
Cryptography	The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (ISO 7498-2)
Cryptography, Approved	Cryptography that has been endorsed by allied nations such as the United States and is proposed for use in specific, documented departmental applications. Approval for use of this cryptography is obtained from CSE. (GSP)
Cryptography, Endorsed	Cryptography that has been evaluated by CSE and considered to meet accepted criteria. This includes hardware, software and firmware implementations of cryptographic algorithms. (GSP)
Data	A representation of facts, concepts or instructions arranged in a formalized manner suitable for telecommunications, interpretation, or processing by humans or by automated means (includes software). (GSP)
Data Base	A repository of data, organized in hierarchical or relational fashion using a specialized file structure, and managed using direct access. A single data base is typically shared among many programs or subsystems, each of which may use a different logical view of the data. (CAG)
Data Contamination; Data Corruption	A deliberate or accidental process or act that results in a change in the integrity of the original data. (AR 380-380; FIPS PUB 39)
Data Integrity	The property that data is being handled as intended and has not been exposed to accidental or intentional modification or destruction. (New)
Dedicated Security Mode	A mode of operation wherein all users have the clearance, formal access approval, and need-to-know for all data handled by the IT system. In the dedicated mode, an IT system may handle a single classification level and/or category of information or a range of classification levels and/or categories. (Based on DODD 5200.28; NCSC-WA-001-85)
Denial of Service	The prevention or delay of legitimate or authorized access, or the unauthorized withholding of critical information or resources. (CIS/01/06)

Departmental Security Officer (DSO)	The individual responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the Security policy and standards. (GSP)
Designated Assets	Assets, other than information, that have been identified by an organization as being important to operations by virtue of the function performed, or as being valuable and therefore warranting safeguarding; for example, cash and other negotiables; and IT systems that require protection to ensure the confidentiality, integrity and availability of the information stored in them. (GSP)
Designated Information	Information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to organizations or individuals outside the national interest. (FASO TRA SIG)
Destruction	The physical alteration of IT system media or IT system components such that they can no longer be used for processing, communications and storage or retrieval of information. This term may also refer to the alteration, modification, deletion, of information or files in such a way that the information is unreadable or absent. (New)
Detection	The process of identifying the occurrence of an event and possibly the agent involved. The purpose of some protective mechanisms. (CSA Vocab.)
Digital Signature	A cryptographic transformation of data which, when appended to a data unit, provides the services of origin authentication, data integrity, and signer non-repudiation. (GSP)
Disclosure	A violation of the security policy of a system in which information has been made available to unauthorized entities. (New)
Discretionary Access Control	A means of restricting access to objects based on the identity and need-to-know of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject or user with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject or user. (NCSC-WA-001-85; CSC-STD-001-83; CSC-STD-004-85)
Domain	The set of objects that a subject, user or resources in an IT system has the ability to access. A domain may also refer to an operational environment. For example, an accounting section of an

	organization could be a domain and access to that domain would be limited to a specific group or individual. (New)
Eavesdropping	A passive attack aimed at compromising the confidentiality of information. (CAG)
Electronic Authorization and Authentication	An electronic means of identifying and verifying the rights or authorities of a legitimate user of a network application (authorization), and of identifying and verifying legitimate application users and devices (authentication). (GSP)
Electronic Funds Transfer (EFT)	Electronic funds transfer refers to the movement of value (money) from one party to another by electronic means. (GAO)
Electronic Mail (E-Mail)	The transmission of letters, messages, memos from one computer to another without using printed copies. (CAG)
Emanation Security	The discipline of reducing electromagnetic interference between information technology and telecommunications equipment, as well as reducing unintentional electro-magnetically radiated signals, that, when intercepted, divulge sensitive information. (GSP)
Emergency Plan	*See Contingency Plan*
Emission Security (EMSEC)	All measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from communications and information systems. (CAG)
Encryption	The transformation of readable data or information into an unreadable stream of alpha/numeric using a reversible coding process. (MG01)
Enhanced Reliability Check	An assessment to determine an individual's trustworthiness; condition for enhanced reliability status. (GSP)Enhanced Reliability Status. The type of personnel screening that, with a need to know, is required for access to designated information and assets. (GSP)
Entrapment	The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or for confusing an intruder about which flaws to exploit. (Adapted from AR 380-380; NCSC-WA-001-85)
Evaluation	The evaluator's report to the Designated Approving Authority

	describing the investigative and test procedures used in the analysis of an IT system's security features with a description and results of tests used to support or refute specific system weaknesses that would permit the acquisition of identifiable classified material from secure or protected data files. (Adapted from DODD 5200.28M)
Event	A change in system state. In general, an event has a trigger, a means or mechanism, and an effect or consequence. An event may be undesirable from a security point of view, in which case it is called a threat event. (MBW2) *See also Threat Event*
Execute	A code or command (e.g., .exe) that commands an application or program to run. (New)
Exposure	The degree to which an asset or group of assets may be exposed to loss, disclosure, destruction or modification, or possibly to undesirable consequences, by the occurrence of one or more threat events. (New)
External Security Audit	A security audit conducted by an organization independent of the one being audited. (FIPS PUB 39)
Extremely Sensitive, Designated Information	A sub-set of designated information that could reasonably be presumed to cause extremely serious injury, such as loss of life, if compromised; may be marked PROTECTED C. (GSP)
Fault	A condition that causes a device or system component to fail to perform in a required manner. (Based on AR 380-380; NCSC-WA-001-85)
Fault Tree Analysis	A technique used in risk assessment that calls for a "what-if" decision to be made at each step of a proposed risk scenario. (Adapted from CSA Vocab.)
Firewall	A software application or an IT system that acts as a security barrier between two network segments and mediates access between those two networks according to an approved set of rules. (New)
Firmware	Software that is permanently stored in a hardware device which allows reading of the software but not writing or modifying. The most common device for firmware is Read Only Memory (ROM). (AFR 205-16)

Flaw	An error of commission, omission, or oversight in an IT system that allows protection mechanisms to be bypassed or disabled. (Adapted from CSC-STD-001-83; NCSC-WA-001-85)
Flaw Hypothesis Methodology	A system analysis and penetration technique where specifications and documentation for the system are analysed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists and, assuming a flaw does exist, on the ease of exploiting it on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system. (CSC-STD-001-83; NCSC-WA-001-85)
Flooding	Accidental or malicious insertion of a large volume of data resulting in denial of service. (Based on 2382-08)
Formal Accreditation	Accreditation granted when the certification/accreditation process has been followed and the residual risk is acceptable to the Departmental Security Officer. (CAG)
Functional Requirement	A stated requirement for an IT system to perform an action or series of actions to accomplish a specific purpose or achieve a specific goal. (CIS/01/6)
Functional Testing	The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation. (NCSC-WA-001-85)
Gateway	A component, normally consisting of hardware and software elements, whose purpose is to control the transfer of information from one IT system or domain to another. (New)
Guideline	A statement indicating a direction which, while not mandatory, should be followed unless there is an compelling reason not to do so. (CAG)
Hacker(s)	All persons, criminal or otherwise, who penetrate computers or communications networks with malicious intent. (New)
Handled	The term "handled by" denotes the activities performed on information in an IT system, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating and controlling. (Based on DODD 5200.28)
Hardware	The electric, electronic, and mechanical equipment used for processing data. (DOE 5636.2A)

Hardware Security	Equipment features or devices used in an IT system to preclude unauthorized access or support a Trusted Computing Base. (Based on NCSC-WA-001-85)
Harm; See also Impact	An expression of the degree and kind of damage, or other change, caused by a consequence. (MBW2)
Hostile Threat Environment	An area that contains known threats and possesses little or no control over the surrounding area such as experienced by some diplomatic facilities. (AFR 205-16)
Hot Site	An alternate processing facility with a skeleton crew, hardware, and sufficient software applications resident at the site so that essential organizational services may be maintained. (New)
Human Asset	Employees, contractors, clients and any others providing services to the organization. (FASO TRA SIG)
Identification	A unique, and perhaps auditable representation of each individual user within an IT system, usually in the form of a string of characters (e.g., LoginID). (New)
Identification Card	A document issued by an organization to identify the bearer as an employee of that organization.
(GSP)Identity-based Security Policy	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. (ISO 7498-2)
Identity Validation; See also Authenticate and Authentication	The performance of tests, such as the checking of a password, that enables an information system to recognize users or resources as identical to those previously described to the system. (WB)
Impact	A measure of the degree of damage or other change caused by a threat event. (**Other**)
Impersonation; Synonymous with Masquerading and Minimizing	An attempt to gain access to an IT system by posing as an authorized user. (Based on FIPS PUB 39)
Incident	*See Computer Security Incident*
Information	Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms,

	whether oral or maintained in any medium, including computerized databases, paper, microfilm, or magnetic tape. Note: Although "data" and similar terms are often used interchangeably with "information", there is a significant distinction. Information is data that have been processed in some way, and information has value where data may have little or even negative value. For example, padding for purposes of defeating traffic or information flow analysis adds data that have a negative value to those interested in the information available from the traffic analysis. (A-130; DODD 5200.28)
Information Asset	Primarily data, but it can also be any other indirect representation of knowledge. For example, an activity or item which may be innocuous in itself, may through inference represent a body of knowledge. (New)
Information Security (INFOSEC)	The application of security measures and safeguards to protect all types of information, processed in any form or operational environment. This includes the handling, storage, manipulation, distribution, or discussion of information processed on paper, in electronic or other technical forms, or verbally. Information Security is an all encompassing term that includes: Physical Security, Personnel Security, Procedural or Administrative Security, Transmission Security, Information Technology Security (ITS) which in itself includes, Computer Security, Network Security, Cryptographic Security, Emission Security. (Adapted from CAG)
Information System	The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. (A-130; DODD 5200.28)
Information Technology (IT)	The scientific, technological and engineering disciplines and the management practices used in electronic information handling, communication and processing; the fields of electronic data processing, telecommunications, electronic networks, and their convergence in systems; applications and associated software and equipment together with their interaction with humans and machines. (GSP)
Information Technology Security (ITS)	The protection resulting from an integrated set of safeguards designed to ensure the confidentiality of information electronically

	stored, processed or transmitted; the integrity of the information and related processes; the accountability of the information stored, processed or transmitted; and the availability of systems and services. (Based on GSP)
Information Warfare	The offensive and defensive use of information and information systems to exploit, corrupt, or destroy, an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military, governments or business interests. (Adapted from ST)
Intangible Asset	The attitude, value or perception impacting the organization, e.g., public confidence, goodwill, competitive advantage, morale, ethics, productivity or loyalty. (FASO TRA SIG)
Integrity	The accuracy and completeness of information and assets and the authenticity of transactions. (GSP) *See also Data Integrity and System Integrity*
Interface	The common boundary between independent systems or system modules where communications take place. (New)
Internal Controls	The assignment of responsibilities to individuals and groups within an organization, and all of the methods and measures adopted by that organization to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency. (Based on A-123; DODD 7040.6)
Interruption	The non-availability of information, assets, systems, or services. Interruption can be accidental or deliberate. (GSP)
IT Security Documentation	Documents which describe an activity's IT security posture and include risk assessment plan and reports, security test and evaluation plans and reports, inspection reports and findings, incident reports, contingency plans and test results, and standard operating procedures. (Adapted from OPNAVINST 5239.1A)
IT Security Policy	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems. (ISO)
IT Storage Media	A physical component, such as a Ahard disk drive@, that is used by an IT system to store application programs and/or information. (New)

IT System	An assembly of computer hardware, firmware, telecommunications, interconnections with other IT equipment (e.g., networks), and the entire collection of software that is executed on that hardware. Included in this definition are word processors, microprocessors, personal computers, controllers, peripherals, or other stand-alone or special computer systems. (Adapted from DOE 5636.2A)
Key	A sequence of symbols that controls the operations of encipherment and decipherment. (ISO 7498-2)
Key Management	Manual and electronic procedures for the generation, dissemination, replacement, storage, and destruction of keys that control encryption or authentication processes. (MG01)
Likelihood	The probability of a given event occurring. (New)
Limited Access; See also Access Control	Limiting access to the resources of a system only to authorized personnel, users, programs, processes, or other systems. (Based on AFR 205-16)
Local Area Network (LAN)	Generally a short-haul communications system that connects IT resources within a defined perimeter, such as a portion or floor of a building, an entire building, or a group of buildings. IT resources include, but are not limited to workstations, front-end processors, controllers, routers, switches, gateways, firewalls and peripherals. (New)
Log	A chronological record of data processing operations. (New)
Logical Access Control	The process of limiting access to resources of an IT system(s) only to authorized users, processes or other systems. (NEW)
Logic Bomb	A resident computer program that lies dormant until a predefined condition is met and which, when executed, checks for particular conditions or particular states of the system which, when satisfied, triggers the perpetration of an unauthorized act. (New)
Login/Log In; Also Logon	Procedure used to establish the identity of the user and the levels of authorization and access permitted to an IT system. (New)
Logoff/Log Off; Also Logout	Procedure used to terminate a connection or a session from an IT system. (New)
Loss	A quantitative measure of harm or deprivation resulting from a compromise. (ISO 2382-08)

Loss of Confidence	The condition of losing faith in the organization's information and/or IT systems. (New)
Loss of Service	The condition of not being able to produce and/or deliver a specific service, or have a required service delayed to the point where it causes interference with normal day-to-day activities. (Other)
Low-sensitive, Designated Information	A sub-set of designated information that could reasonably be presumed to cause injury if compromised; may be marked PROTECTED A. (GSP)
Malicious Logic	Hardware, firmware or software that are intentionally included in, or introduced into, an IT system for an unauthorized purpose; e.g. Trojan Horse, Virus, Worm. (CIS/01/6)
Mandatory Access Control	A means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization of subjects to access objects of such sensitivity. Note that the ability to grant or revoke access is governed by organizational security policy not object ownership. (Based on CIS/01/6)
Masquerade or Masquerading	*See Impersonation*
Material Asset	A physical item of some value. This may include but is not limited to buildings or facilities within, accommodations, furniture, supplies and IT equipment and/or systems. (New)
Maximum Permissible Downtime (MPD)	The maximum period of time for which the system (or a component of the system) can be unavailable. The MPD is a function of the frequency with which reports are generated by the system, the response time demanded for information requests, and the amount of data that must be entered into the system for any period of time. (New)
Means	The mechanism or medium that is used by a threat agent in the occurrence of a threat event. (Based on MBW2)
Mechanism	A system entry point or separate system support program that performs a specific action or related group of actions. (Based on NIST Vocab.)
Mode(s) of Operation	A way of categorizing IT systems with respect to the controls that

	are needed to enforce the security policy requirements for appropriate security clearance/screening and need-to-know. The 3 modes are: Dedicated, System High and Multi-level. Modes of operation may also refer to cryptography, where an encryption algorithm may be implemented in different ways. For example, the DES algorithm has four modes, one of which is Electronic Code Book (ECB). (New)
Modification	The accidental or deliberate alteration of information, data, software or IT system equipment. (GSP)
Monitor or Monitoring	To ensure that information and assets, or the safeguards protecting them, are checked by the personnel in control of the information or assets, security staff or electronic means with sufficient regularity to satisfy the threat and risk assessment. (GSP)
Motivation	Something that induces a threat agent to act against a system. (MG03)
Multilevel Mode	A Mode of operation of an IT system where all users do not have an appropriate personnel screening level or need-to know for all information contained in that system. This mode of operation requires a high degree of trustworthy security functionality in the IT system; in some cases these requirements may exceed the type of trusted IT systems available in the marketplace. (New)
National Interest	Concerns the defence and maintenance of the social, political and economic stability of a nation, and thereby the security of the nation. (Based on GSP)
Need-to-access Principle	The necessity for limiting access to a specific area to those who need to work there. (GSP)
Need-to-know Principle	The necessity for limiting access to knowledge of, or possession of certain information and material to those whose duties require such access. (New)
Network	A communications medium and all components attached to that medium that are responsible for the transfer of data between communicating stations (entities). (New)
Object	A passive entity within an IT system that contains or receives information. Access to an object potentially implies access to the information it contains. Note that a program may be considered an object, but once activated becomes a subject. (CIS/01/6)

Open Security Environment	An environment that includes those systems in which one of the following conditions holds true: (a) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (b) Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications. (CSC-STD-004-85; CSC-STD-003-85; NCSC-WA-001-85)
Operating System	An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or output, accounting, resource allocation, storage assignment tasks, and other system related functions. (DODD 5200.28M)
Operational Data Security	The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations. (AR 380-380; NCSC-WA-001-85)
Operations Environment	An area that is under the control of computer operations personnel. (GSP)
Output	Information that has been exported by an IT system. (New)
Overwrite	A procedure to remove or destroy data recorded on magnetic storage media by writing patterns of data over top of that data. (Based on NCSC-WA-001-85)
Packet Filter	A device which will allow or deny data packets to cross an IT network boundary. The allow/deny decision is based upon a set of filtering rules which are determined by the IT Network Security Policy. (New)
Particularly Sensitive, Designated Information	A sub-set of designated information that could reasonably be expected to cause serious injury if compromised; may be marked PROTECTED B. (GSP)
Passive Threat	The threat of unauthorized disclosure of information without changing the state of the system (e.g.: the recovery of sensitive information by the interception of data transmission). (Based on ISO 7498-2)
Password	Private authentication information, usually composed of a string of

	characters. Depending upon system design and/or implementation, knowledge of a valid user ID and its associated password may be considered proof of authorization to access IT systems or networks. (New)
Penetration	The successful unauthorized access to an IT system. (New)
Permissions	A description of the type of authorized interactions a subject can have with an object. Permissions include: read, write, execute, add, modify, and delete. (AFR 205-16; NCSC-WA-001-85)
Personal Information	Any form of recorded information about an identifiable individual. See Section 3 of the Privacy Act for examples. The Act also includes some exceptions to the definition. Personal information, a subset of other sensitive information, deserves enhanced protection and may carry the marking "PROTECTED personal information". (GSP)
Personnel Security	The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances. (FIPS PUB 39; AR 380-380; NCSC-WA-001-85)
Physical Security	The application of physical barriers and control procedures to provide protection, detection and response mechanisms used in the physical environment to control access to sensitive information and assets. (New)
Piggy Back	The gaining of unauthorized access to an IT system or network via another user's legitimate connection. (MG01)
Policy; See also Security Policy	An approved top level statement with a set of rules or plan of action for the purpose of maintaining appropriate security for the organization. (New)
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security. (ISO 7498-2)
Procedural Security	Approved management constraints; operational, administrative, and accountability procedures; and other supplemental controls established to provide protection for sensitive information. (Based on AR 380-380)

Procedure	An approved course of action to accomplish an objective, that may require accountability, conformance and adherence to a security policy. (Based on CIS/01/6) *See also Backup, and Recovery Procedure(s)*
Product Assessment	A process by which The Communications Security Establishment (CSE) examines the security features of an IT security product or system that is now operating, or is intended to operate, in a specific environment and application to determine the degree to which the implemented security features meet a defined security requirement or to enforce the security policy. The results of an assessment is limited to the implemented security features of the product or systems for a defined application and/or environment; any changes either to the version product, application or environment may negate the results of the assessment. (New)
Product Endorsement	A product endorsement is a public pronouncement by The Communications Security Establishment (CSE) stating that an IT security product or system(s) was evaluated and found to meet a specific set of criteria and that the product's proper installation, implementation and continuous configuration control will provide the required security within the boundaries of the criteria against which it was evaluated. An endorsement may be stated in a form of a rating; for example, a trusted system evaluated against the Common Criteria may receive a assurance level rating of AL3. (New)
Product Evaluation	The process by which The Communications Security Establishment (CSE) methodically investigates the security properties of an IT security product and/or system(s) against a set of criteria. If the product or system(s) meets a specific set of criteria, that product is eligible for endorsement by CSE. (New)
Product Review	The process by which The Communications Security Establishment (CSE) reviews the standard product or system documentation to determine whether the product performs the security functions as stated when it is installed in accordance with the documentation. A product review will identify obvious flaws and misrepresentations and provide an objective and impartial analysis. This analysis may be considered adequate for an application where a Threat and Risk Assessment has failed to identify a threat of any consequence. A product review may also be used to select a suitable candidate, a product assessment or evaluation from a host of similar IT security products or systems. (New)

PROTECTED	The marking that shows that the information qualifies as designated information and requires more than basic protection. (GSP)
Protection Mechanisms	*See Security Features*
Protocol	A set of rules and formats that permits entities to exchange information. (CIS/01/6)
Public Key Cryptography	*See Asymmetric Cryptography*
Read Access	A software command which grants a user the privilege to open a file and read its contents. The user cannot add to or modify the file. (New)
Recovery Procedure(s)	The actions necessary to restore a system's computational capability and data files after a system failure or penetration. (FIPS PUB 39; AR 380-380; NCSC-WA-001-85)
Red	A method of identifying an IT resource or system and its associated communications medium that is processing or handling sensitive or classified information. (New)
Reliability	The property of an IT system to maintain consistent, intended and trustworthy operation over a given period of time. (New)
Remote Access	A method by which a user in one location, such as the home, may gain access to that user's organization IT resources or system normally via some commercial means such as telephone service providers. For example, an employee may, using a modem and the home telephone service, dial into his or her organization's IT resources; that is, if that organization's IT resources are provisioned for such a capability. (New)
Replacement Cost	The actual expenditure required to replace the asset(s). Some of the elements that contribute to the overall costs are, time to operation, direct purchase costs, installation and training costs. (New)
Repudiation	Denial by one of the entities involved in a communication of having participated in all or part of the communication. (ISO 7498-2)
Residual Data	Data left in a data medium after deletion of a file or a portion of a file. Note: This data remains recoverable until sanitizing of the data medium has taken place. (Other)

Residual Risk	The risk that remains after safeguards have been selected and implemented. (TSEG)
Resources (Characteristic of Threat Agent)	The equipment, money, people, knowledge, etc. available to a threat agent to initiate an attack. (MG03)
Restoration Priority	The order in which IT processing support is allocated to IT systems during disaster or emergency conditions. (CAG)
Restricted Area	Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property, material or information.(New)
Risk	Intuitively, the adverse effects that can result if a vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences. There is no standard definition. (Based on Computer Related Risks)
Risk Acceptance	An action taken by the responsible manager to declare and be held accountable for acceptance of the remaining or residual risks attributed to an IT system after the performance of a threat and risk assessment. Generally, the acceptance of the residual risk is made because any further addition of safeguards does not justify the effort in terms of cost or functionality. (New)
Risk Assessment	An evaluation of risk based on threat assessment information, the effectiveness of existing and proposed security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets. (New)
Risk Management	The process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost. (MG01)
Risk Management Program	A program designed to ensure that critical decisions regarding the adequacy of IT system security safeguards are made by authorized managers based on established risk management techniques. (New)
Safeguard(s)	The approved minimum security measure(s) and controls which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(ies) which would compromise an IT system. (Based on MG02)

Sanitization; Sanitizing	Altering or erasing, by electronic means, recorded sensitive information to prevent unauthorized disclosure. (Based on GSP)
Scenario Analysis	An IT system vulnerability assessment technique in which various possible attack methods are identified and the existing safeguards are examined in light of their ability to counter such attack methods. (Based on WB)
Secret	Level of classification that applies to information or assets when compromise could reasonably be expected to cause serious injury to the national interest. (GSP)
Secret Key	A key that is intended for use by a limited number of correspondents for the encryption and decryption of information using symmetric algorithms. (Symmetric cryptography refers to the technique where the same key and device are used for encryption and decryption of information between 2 or more correspondents.) Unauthorized access to the key could compromise the security provided by the encryption devices, hence, the necessity to keep the key secret and accessible to authorized users. (New)
Secure Operating System	An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system. (FIPS PUB 39; AR 380-380)
Secure Perimeter	Continuous physical barriers that can reasonably be expected to counter identified threats.(GSP)
Secure Zone	An area, normally located in a restricted area, in which is housed highly sensitive equipment and information, to which access is restricted to authorized persons. (CSA Vocab.)
Security Architecture	A system-specific set of complementary operational, procedural and technical security measures selected and organized in a logical and effective manner to protect the confidentiality, integrity and availability of system assets at a level determined through risk assessment and accepted by the responsible user as advised by the security authority. (CIS/01/6)
Security Audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy and procedures. (ISO 7498-2)

Security Breach	A violation of controls of a particular information system such that information assets or system components are unduly exposed. WB)
Security Classification	The determination of which specific degree of protection against disclosure the information requires, together with a designation of that degree of protection (e.g., top secret, secret, confidential). (ISO 2382-08)
Security Clearance	The type of personnel screening that, with a need to know, is required for access to classified information and assets. (GSP)
Security Domain	A system subset that exists in a substantially different environment from other components, contains information that is subject to different controls or which executes on hardware and software with different vulnerabilities and requires some unique form of protection to the information and/or processes which it contains. (New)
Security Evaluation;	One of two types of evaluations done to assess the degree of trust that can be placed in IT systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing an IT system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process. (Based on NCSC-WA-001-85) *Synonymous with Security Assessment*
Security Fault Analysis	A security analysis performed on a hardware device to determine the security properties of the device when a hardware fault is encountered. (New)
Security Features	The security relevant functions, mechanisms, and characteristics of IT system hardware and software. Security features are a subset of IT system security safeguards. (Based on NCSC-WA-001-85; DODD 5200.28)
Security Filter	A secure subsystem that enforces the IT security policy on the data that passes through it. (New)
Security Function	An action or set of actions performed by an element of an IT system to enforce some aspect of the system security policy. (CIS/01/6)

Security Measures	Elements of software, firmware, hardware, or procedures that are included in the system for the satisfaction of security specifications. (AFR 206-16; NCSC-WA-001-85)
Security Mode	A level of security in which the Designated Approving Authority accredits an IT system to operate. Inherent with each of the security modes are restrictions on the user clearance levels, formal access requirements, need-to-know requirements and the range of sensitive information permitted on the IT system. (Adapted from NCSC-WA-001-85; DODD 5200.28)
Security Officer	A person who is made responsible for the overall security of an IT system. Note: The security officer will normally consider physical, personnel and procedural security.
Security Perimeter; Synonymous with Control Zone	The physical boundary where security controls are in effect to protect assets. (Based on NCSC-WA-001-85)
Security Policy	The set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information, and how it manages and controls the use of critical resources. The security policy is made specific to an IT system in its Statement of System Security Requirements. (CIS/01/6)
Security Policy Model	An abstract representation of the system security policy. The representation may be in the form of a formal mathematical model, a natural language description of the working of the model or a combination of the two. (CIS/01/6)
Security Requirement(s)	The specification of a security function(s) needed within an IT system, which if satisfied will result in the IT system meeting its Target Residual Risk. (Based on CIS/01/6)
Security Requirements Baseline	A description of minimum security requirements necessary for an IT system to maintain an acceptable level of security. (Based on NCSC-WA-001-85)
Security Safeguards	*See Safeguards*
Security Service	A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. (ISO 7498-2)

Security Testing	A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application's environment. This process includes hands-on functional testing, penetration testing, and verification. (CSC-STD-001-83; NCSC-WA-001-85)
Security Test and Evaluation (ST&E)	The process to determine that the system's administrative, technical, and physical security measures are adequate for the system; to document and report test findings to appropriate authorities; and to make recommendations based on test results. Managers may choose to conduct the ST&E as an integral part of other tests and evaluations. They must ensure changes made to correct one problem do not adversely affect other previously tested security measures. (AFR 206-16; OPNAVINST 5239.1A)
Security Validation	The process of determining whether the system security features implement the organizational and system specific security policy. (MG01)
Security Verification	The process of determining whether technical and non-technical safeguards are implemented correctly and meet assurance requirements. (MG01)
Security Violation	An instance in which a user or other persons, unintentionally or intentionally, circumvent or defeat the controls of a system that will permit the suspected or actual compromise of sensitive assets. (New)
Sensitive	*See Sensitive Asset*
Sensitive Application	An application that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application. (Based on A-130)
Sensitive Asset	An asset that, as determined by the Designated Approving Authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will cause perceivable damage to someone or something.
Sensitive Data	*See Sensitive Asset and Sensitive Information*
Sensitive Discussion Area (SDA)	Specially designed and managed area to prevent the overhearing, by electronic or other methods, of discussions on classified and

	designated information. (GSP)
Sensitive Information	Information that requires protection due to the risk of loss or harm that could result from inadvertent or deliberate disclosure, modification, or destruction. The term includes information classified in one of the three security classification categories as well as information about individuals requiring protection under the Privacy Act and information not releasable under the Access to Information Act. (CIS/01/6)
Sensitivity	The characteristic of a resource which implies its value or importance to an organization, or the injury or harm that could result from its deliberate or inadvertent disclosure, modification, loss or denial. (New)
Sensitivity Assessment	The evaluation of the information and IT resources to determine their vulnerability in terms of confidentiality, integrity, availability and accountability.(New)
Severity	A measure of the degree of damage suffered as the result of an event. May be expressed as a percentage of the impacted assets or as a time interval. (CSA Vocab.)
Signature	See Digital Signature
Single-event Loss Expectancy (SLE)	A risk assessment measure which indicates the loss incurred for a single occurrence of a threat scenario. (MG02)
Site-access Security Clearance	Type of personnel screening required in limited and specific circumstances when duties of individuals require access to only sensitive government-related sites or facilities, usually for a short time, and not to information. GSP)
Software	Computer programs, procedures, rules and any associated documentation concerned with the operation of an information processing system. (Based on CAG)
Software Maintenance	Activity intended to retain software in, or restore it to, a state in which it can perform its required function. Software maintenance comprises corrective, adaptive, and perfective software maintenance. (CAG)
Software Piracy	The unauthorized use, copying, or distribution of software products.(ISO 2382-08)

Spoof; Spoofing	The deliberate act of inducing a user or a resource into taking an incorrect action. (CSA Vocab.)
Standard	A statement or set of statements established or made by authority, custom or common consent to serve as a reference model or rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. (Adapted from CIS/01/6)
State	A description of the system assets, threats, security safeguards, and their environment, when a given set of conditions holds. State descriptions are useful for modelling changes that occur between one state and another. (MBW2)
Statement of Sensitivity (SoS)	A description of the confidentiality, integrity and/or availability requirements associated with the information or assets stored or processed in or transmitted by an IT system. (GSP)
Subject	An active entity, generally in the form of a person, process or device that causes information to flow between entities within an IT system, changes the observable properties of the entities, or changes the system state. (CIS/01/6)
Supporting Asset	System components which support the primary assets. Supporting assets may include hardware, software, interfaces, personnel, supporting systems & utilities and access control measures. (MG03)
System	A set of elements such as personnel, physical, environment, safeguards, technology, etc. that are combined together to fulfill a specified purpose or mission. (MG03)
System High Security Mode	A mode of operation in which all users are cleared to see all of the information, but not all users have a need-to-know to carry out their duties. How strictly the need-to-know must be enforced will determine the access controls required. The determination is a function of the potential impact if need-to-know is not maintained. In some situations where special precautions are required, it may be more appropriate to use Multilevel Mode rather than System High mode. (TSEG)
System Integrity	The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system. (ISO)

System/Network Manager	A person assigned the responsibility for the day-to-day operations, configuration control and maintenance of an IT system or network. (CIS/01/6)
System Security Officer (SSO)	The person responsible for the security of an IT system and having the authority to enforce the security safeguards on all others who have access to the system from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. (New)
Tampering	An unauthorized modification which alters the proper functioning of an IT system or piece of equipment in a manner which degrades the security it provides. (Based on NCSC-WA-001-85)
Target	The objective of a hostile threat agent. (MBW2)
Target Residual Risk	The risk to the system which can be accepted and managed by the system operational authority. Based upon risks identified by the risk assessment, it categorizes risks as those which can be accepted as manageable by the system operational authority, and those risks which must be reduced in order to be accepted. In the latter case the level to which risk must be reduced is identified. (CIS/01/6)
TCP/IP	Transmission Protocol over Internet Protocol in use within the Internet. It is roughly equivalent to transport class 4 in the OSI architecture. (Computer Related Risks)
Technical Vulnerability	A hardware, firmware, communication, or software feature, attribute or flaw which may leave an IT system open for potential exploitation either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. (Based on NCSC-WA-001-85)
Telecommunications	As defined in the Interpretation Act, Chapter I-21 of the Revised Statutes of Canada, any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic systems. This includes telephone, telegraph, teletype, facsimile, data transmissions, closed circuit television and remote dictation systems. (GSP)
TEMPEST	The discipline that deals with the suppression of unintentionally radiated or conducted electromagnetic signals that divulge information. (GSP)
Threat	Any potential event or act that could cause one or more of the

	following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.(MG01)
Threat Agent	An entity that may act to cause a threat event to occur by exploiting the vulnerability(ies) in an IT system. (New)
Threat Analysis	The examination of all actions and events for determining the areas of vulnerability and the result of countermeasures to counteract perceived threats to assets that might adversely effect an IT system. (New)
Threat Assessment	An evaluation of threat agent characteristics including resources, motivation, intent, capability, opportunity, likelihood and consequence of acts that could place sensitive information and assets at risk. (New)
Threat Capability	The ability of a threat agent to act, or to be effective. (MG02)
Threat Consequence	The adverse outcome or effect of a threat event on an asset. (FASO TRA SIG)
Threat Event	An event whose occurrence would cause harm to an IT system in the form of disclosure, modification of data, destruction and/or denial of service. (CIS/01/6)
Threat and Risk Assessment (TRA)	A process in which the objective is to identify system assets, to identify how these assets can be compromised by threat agents, to assess the level of risk that the threat agents pose to the assets and recommend the necessary safeguards in order to mitigate effects of the threat agents. (New) *Also, see Threat Assessment and Risk Assessment*
Threat Scenario	A postulated set of circumstances in which a specific threat agent can mount a specific type of attack in an attempt to compromise (in one or more ways) one or more system assets. (New)
Token	A security object containing a set of security credentials. Its is exchanged between to parties who are trying to establish a secure communication channel. (Computer Related Risks)
Top Secret	A level of classification that applies to information or assets which, when compromised, could reasonably be expected to cause exceptionally grave injury to the national interest. (Based on GSP)

Transmission Security (TRANSEC)	That component of COMSEC which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (CIS/01/6)
Trap door	An undocumented and perhaps hidden software or hardware mechanism intentionally created in an IT system that permits system protection mechanisms to be circumvented for the purpose of collecting, altering or destroying data. (New)
Trojan Horse	A computer program that is an apparently or actually useful function that contains hidden additional functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. (MG01)
Trust	Belief that an IT system meets its stated security requirements. (CIS/01/6)
Trusted Computing Base (TCB)	The totality of protection mechanisms within a computer system - including hardware, firmware and software - the combination of which is responsible for enforcing a security policy. (CIS/01/6)
Trusted System	An accredited IT system employing sufficient integrity measures to allow its use for processing sensitive information. (New)
Trusted Third Party	A security authority, or its agent, trusted by other entities with respect to security-related activities. (ISO 9798-1)
Unclassified Information	Property or information which is neither classified nor designated. (CAG)
User	The entity that is identified by the UserID, authenticated prior to system access, the subject of all access control decisions, and held accountable via the audit reporting system. (Based on NIST Vocab.)
User Community	The entities who interact directly with a computer system, usually in sub-groups of end-users, managers, system administrators, developers and application administrators. (Based on Other)
Validation	The performance of tests and evaluations of IT systems or security products in order to determine compliance with security specifications and requirements. (Based on FIPS PUB 39)

Value (Attribute of Asset)	A measure or statement of the utility (usefulness) of an asset or information, or (alternatively) the cost if it is compromised. The value can be stated in quantitative or qualitative terms. Utility and cost are contextually dependent, based on the needs and situation of the organization. Value is therefore not necessarily an objective term. (MBW2)
Verify; Verification	The process of comparing the product of an activity with the requirements or specifications for that activity (e.g.: the comparison of a specification with a security policy model or the comparison of object code with a source code). (ISO 2382-08)
Violation of Security	Any act or omission that contravenes any provision of the Security policy. Such acts may include failure to classify or designate information in accordance with the policy; classification or designation, or continuation of same, in violation of the policy; unauthorized modification, retention, destruction or removal of sensitive information; and unauthorized interruption of the flow of sensitive information. (GSP)
Virus	Pieces of code that adds itself to other programs, including operating systems, but cannot run independently, requiring the host program to activate it. It has three parts; a replication mechanism, a payload and a trigger. The main difference between a Trojan horse and a virus is that a virus is capable of reproducing itself. (CAG)
Vulnerability	A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs. (New)
Vulnerability Assessment	An evaluation of the vulnerabilities of an IT component, program or system to determine if the controls in place or the proposed controls are sufficient to address security issues that could impact the confidentiality, integrity, or availability of the component(s) , program(s) or system(s) assets. (New)
Wiretapping	The monitoring and/or recording of data which is being transmitted over a communication link. This action is considered a passive attack in that there is no intent to interfere with the communications. (MG01)
Worm(s)	A program that scans an IT system or an entire network for available, unused hard disk space in which to run. Worms tend to tie up all computer resources in a system or a network and

	effectively shut it down. (New)
Write	A fundamental operation that results only in the flow of information from one entity to another entity (to append, modify, delete, or create). (New)
Write Access	A privilege granted to a user in which that user has the right to access to a file and be able to append, modify, delete or create new information for that file. (New)

ANNEX L – GLOSSARY SOURCES

Each definition is followed by a corresponding reference from which it was obtained.

A-123	Office of Management and Budget Circular A-123, Internal Control Systems
A-130	Office of Management and Budget Circular A-130, Internal Control Systems
AMSG 524	NATO Glossary of Communications Security Terminology
CAG	(A-IM-100-000/AG-001) Certification and Accreditation of Information Systems - Glossary
CIS/01/6	Information Technology , Security Architecture Handbook, Volume 1 (Interim)
CSA Vocab.	Canadian Standards Association Vocabulary
CSC-STD-001-83	DOD Trusted Computer System Evaluation Criteria
CSC-STD-002-85	DOD Password Management Guideline
DOE 5636.2A	Department of Energy Order 5636.2A, Security Requirements for Classified Automated Data Processing Systems
FASO TRA SIG	Federal Association of Security Officers; Glossary of TRA Terminology
GSP	Government of Canada Security Policy, June 1994
ISO 2382-08	ISO/IEC JTC1/SC1 Information Technology - Vocabulary, 2382-08, ASecurity@
ISO 7498-2	International Organization for Standardization, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2
ISO/IEC 11770-1	Information Technology - Security Techniques - Key Management, Part 1: Framework
MBW2	Proceedings, Second Risk Management Model Builders Workshop, Ottawa, June 1989
MG01	Network Security, Analysis and Implementation, CSE, 1996
MG02	A Guide to Security Risk Management for Information Technology, CSE,

	1996
MG03	A Guide to Risk Assessment and Safeguard Selection for Information Technology, CSE, 1996
MTR-8201	Mitre Corporation Technical Report MTR-8201, Trusted Computer Systems - Glossary
NCSC	(NCSC-WA-001-85) National Computer Security Center, COMPUSECese: Computer Security Glossary
New	New Definition
OPNAVINST	(OPNAVINST 5239.1A) Office of Navy operations Instruction 5239.1A, Department of the Navy Electronic Data Processing Security Program
TSEG	CSE, Trusted Systems Environment Guideline, December 1992; CID/09/17